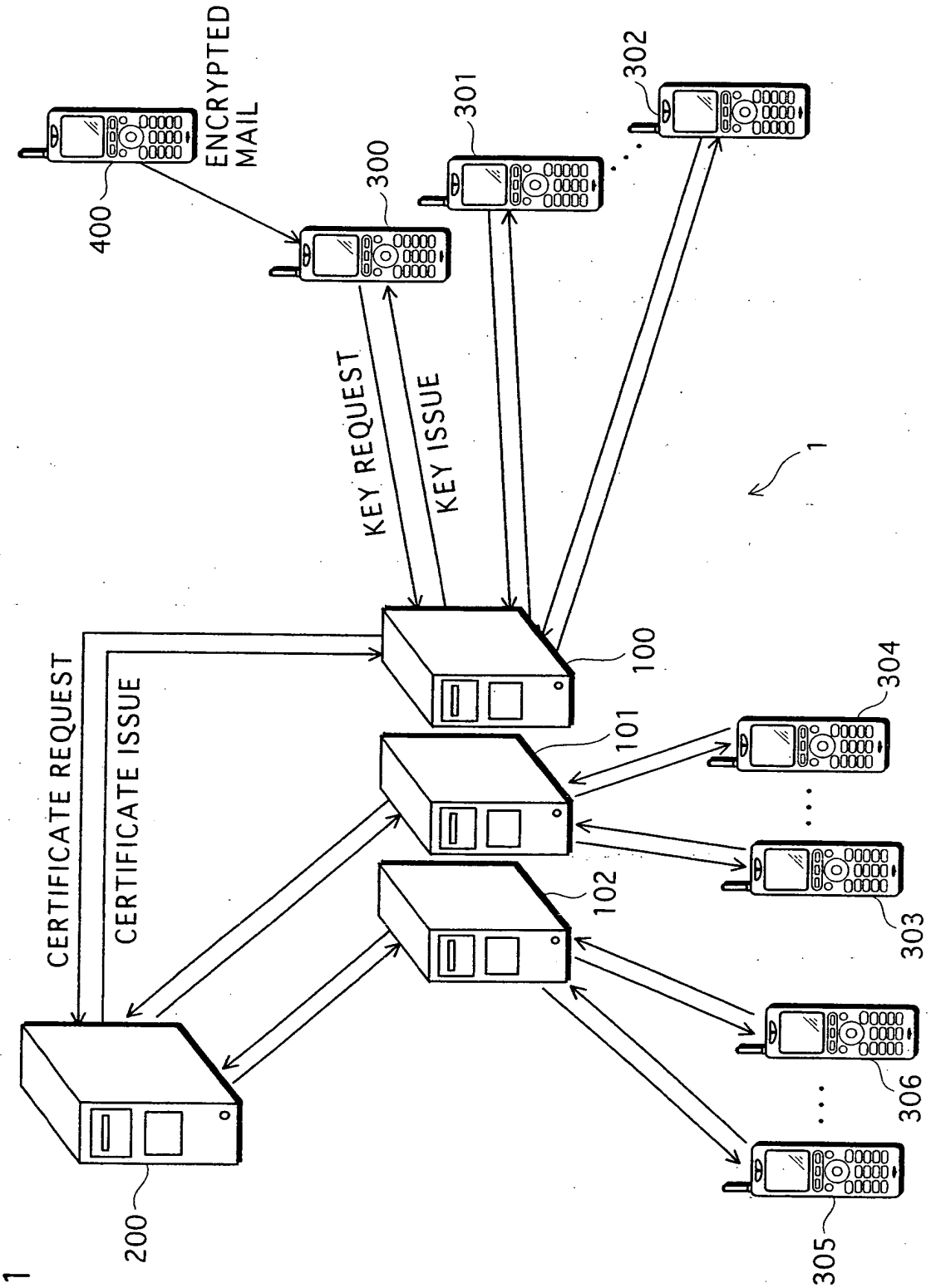

ENCRYPTED MAIL
400
300
301
302
KEY REQUEST
KEY ISSUE
1
CERTIFICATE REQUEST
CERTIFICATE ISSUE
100
101
102
200
304
303
306
305

FIG.1

FIG.2

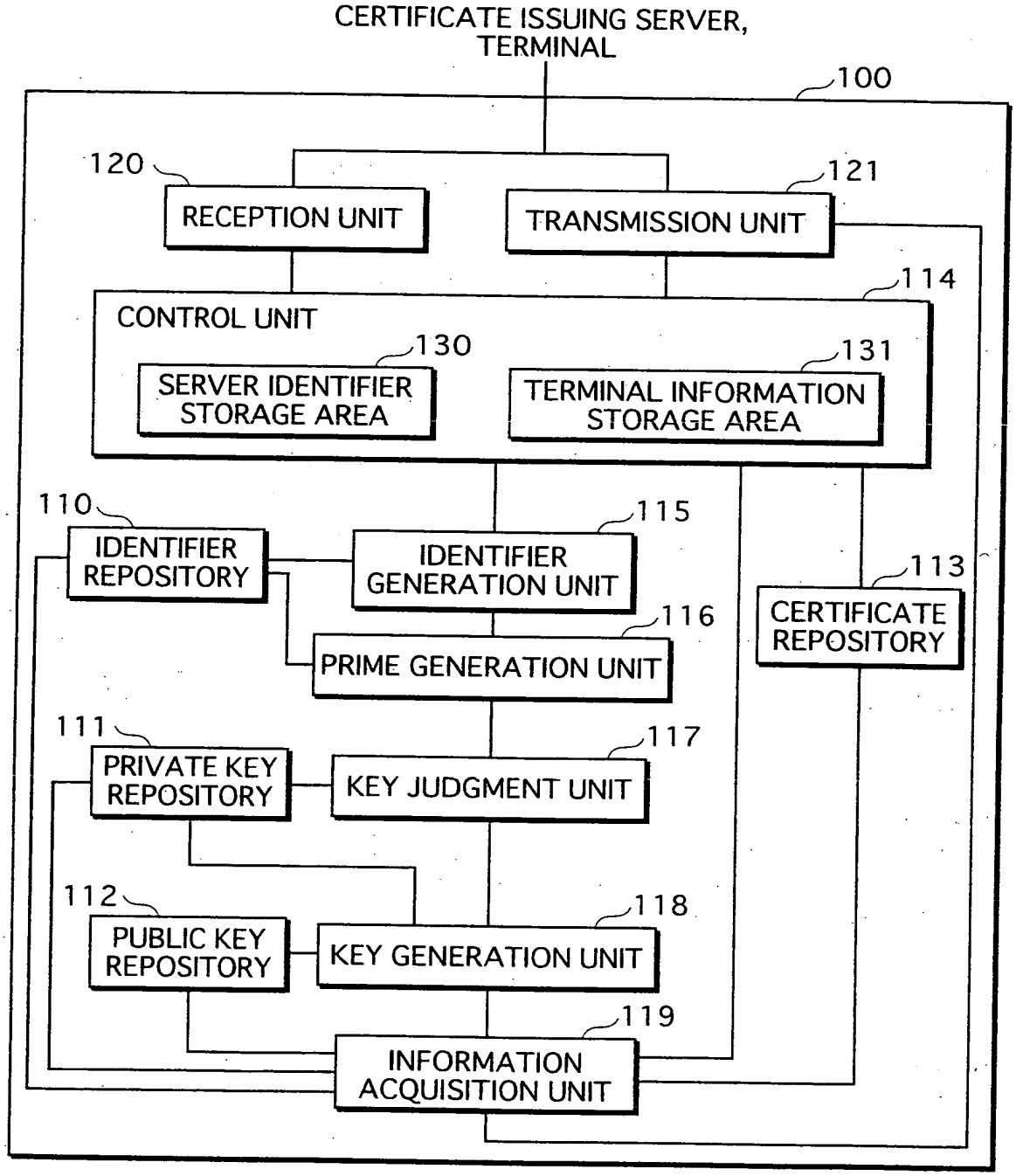

CERTIFICATE ISSUING SERVER, TERMINAL
100
120
RECEPTION UNIT
121
TRANSMISSION UNIT
114
CONTROL UNIT
130
SERVER IDENTIFIER STORAGE AREA
131
TERMINAL INFORMATION STORAGE AREA
110
IDENTIFIER REPOSITORY
115
IDENTIFIER GENERATION UNIT
113
CERTIFICATE REPOSITORY
116
PRIME GENERATION UNIT
111
PRIVATE KEY REPOSITORY
117
KEY JUDGMENT UNIT
112
PUBLIC KEY REPOSITORY
118
KEY GENERATION UNIT
119
INFORMATION ACQUISITION UNIT

FIG.3

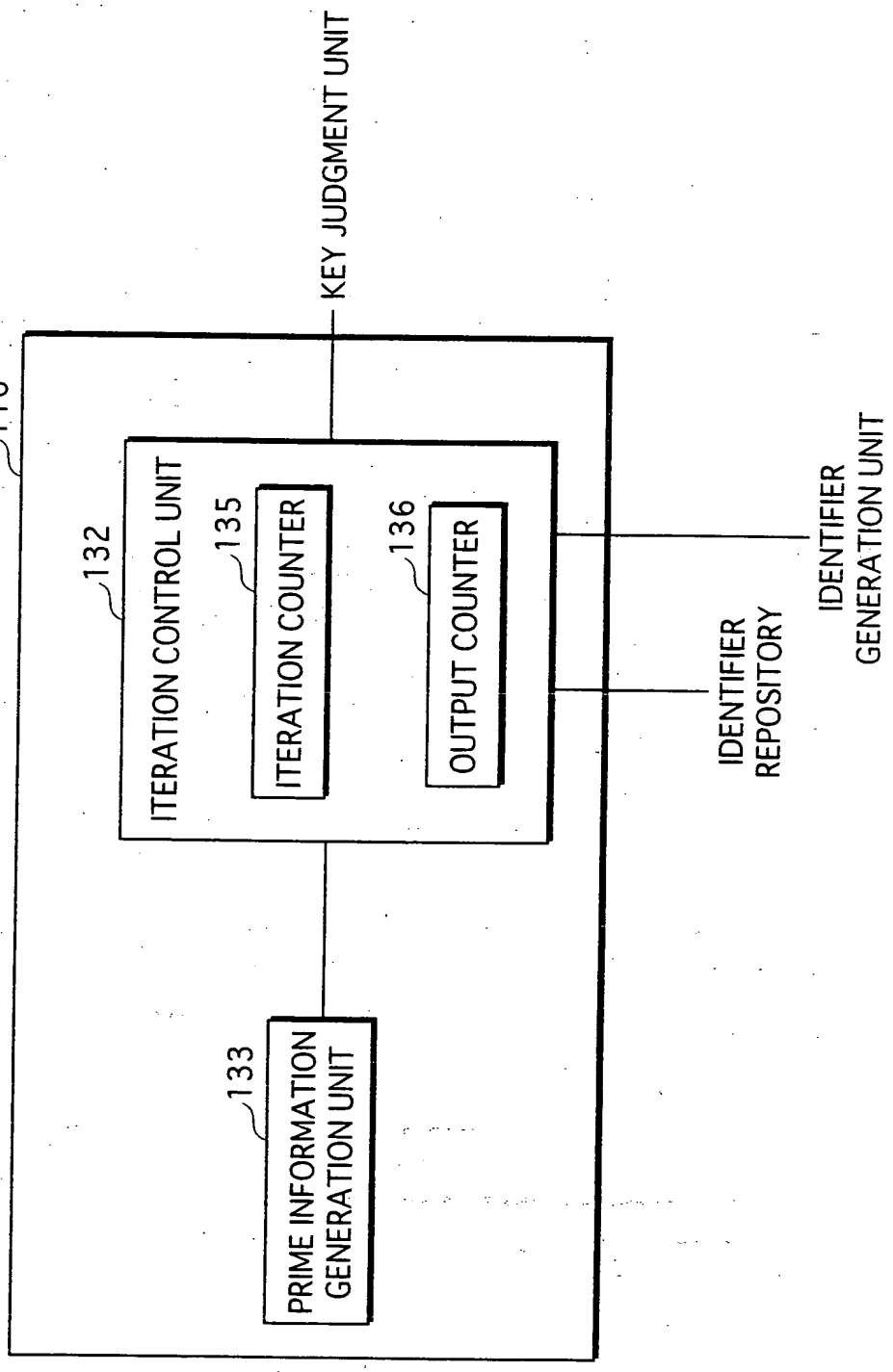

KEY JUDGMENT UNIT
116
ITERATION CONTROL UNIT
132
ITERATION COUNTER
135
OUTPUT COUNTER
136
PRIME INFORMATION GENERATION UNIT
133
IDENTIFIER REPOSITORY
IDENTIFIER GENERATION UNIT

FIG.4

T100

NUMBER OF ITERATIONS	CONTROL INFORMATION
1	INFORMATION C
2	INFORMATION C
3	INFORMATION C
4	INFORMATION C
5	INFORMATION B
6	INFORMATION A

FIG.5

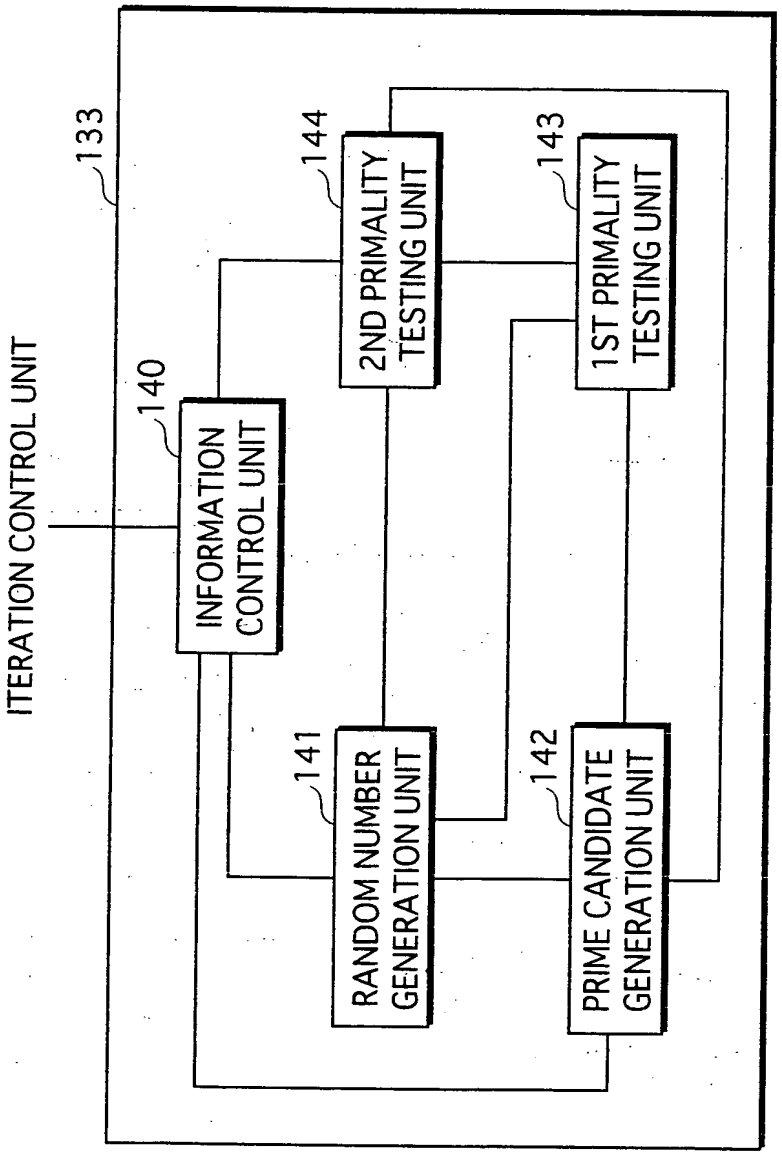

ITERATION CONTROL UNIT
133
140
INFORMATION CONTROL UNIT
144
2ND PRIMALITY TESTING UNIT
143
1ST PRIMALITY TESTING UNIT
141
RANDOM NUMBER GENERATION UNIT
142
PRIME CANDIDATE GENERATION UNIT

FIG.6

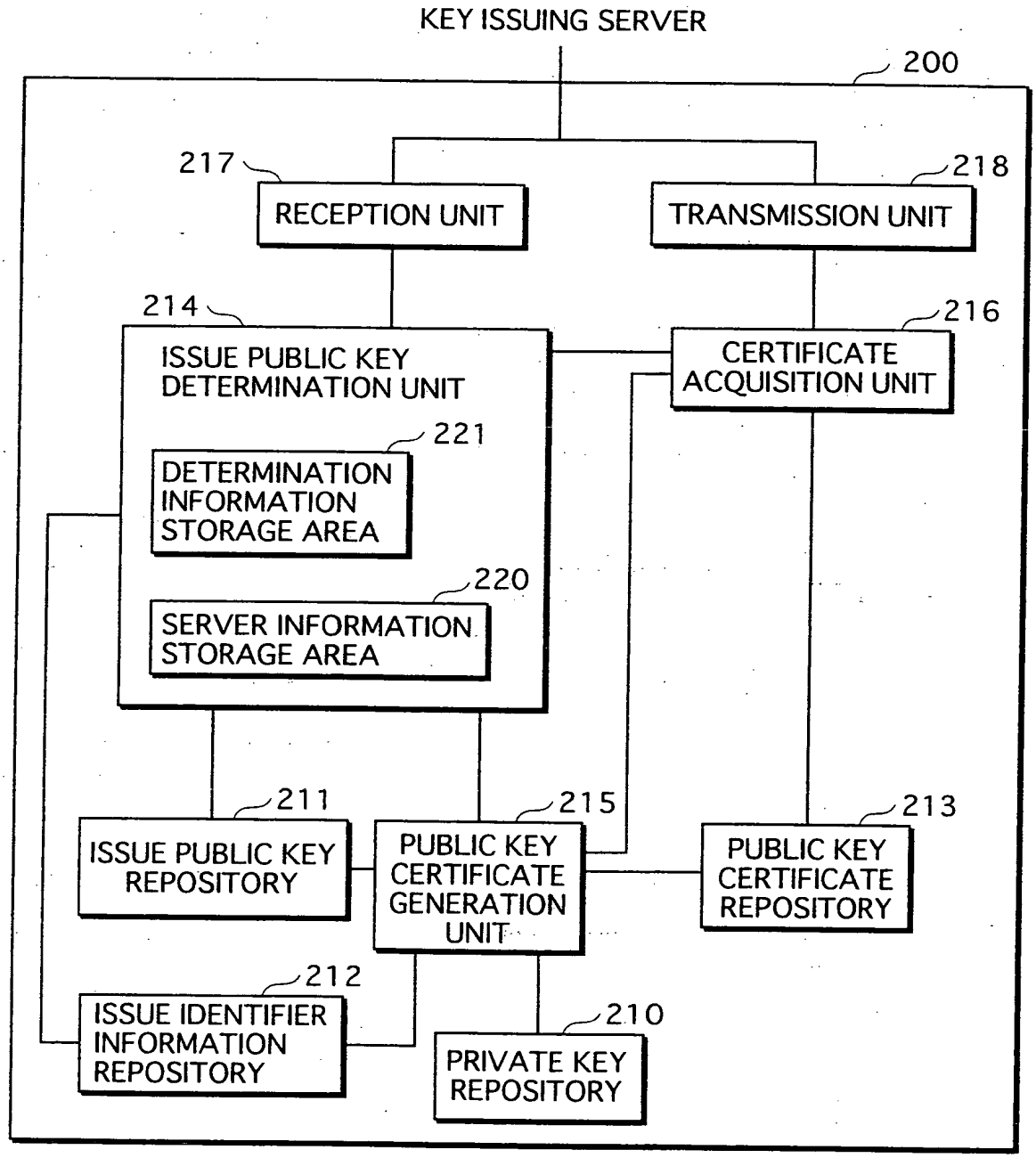

KEY ISSUING SERVER
200
217
RECEPTION UNIT
218
TRANSMISSION UNIT
214
ISSUE PUBLIC KEY DETERMINATION UNIT
216
CERTIFICATE ACQUISITION UNIT
221
DETERMINATION INFORMATION STORAGE AREA
220
SERVER INFORMATION STORAGE AREA
211
ISSUE PUBLIC KEY REPOSITORY
215
PUBLIC KEY CERTIFICATE GENERATION UNIT
213
PUBLIC KEY CERTIFICATE REPOSITORY
212
ISSUE IDENTIFIER INFORMATION REPOSITORY
210
PRIVATE KEY REPOSITORY

FIG.7

T200

SERVER IDENTIFIER	1ST VERIFICATION VALUE	2ND VERIFICATION VALUE
SID A	c11	c12
SID B	c21	c22
SID C	c31	c33

FIG.8

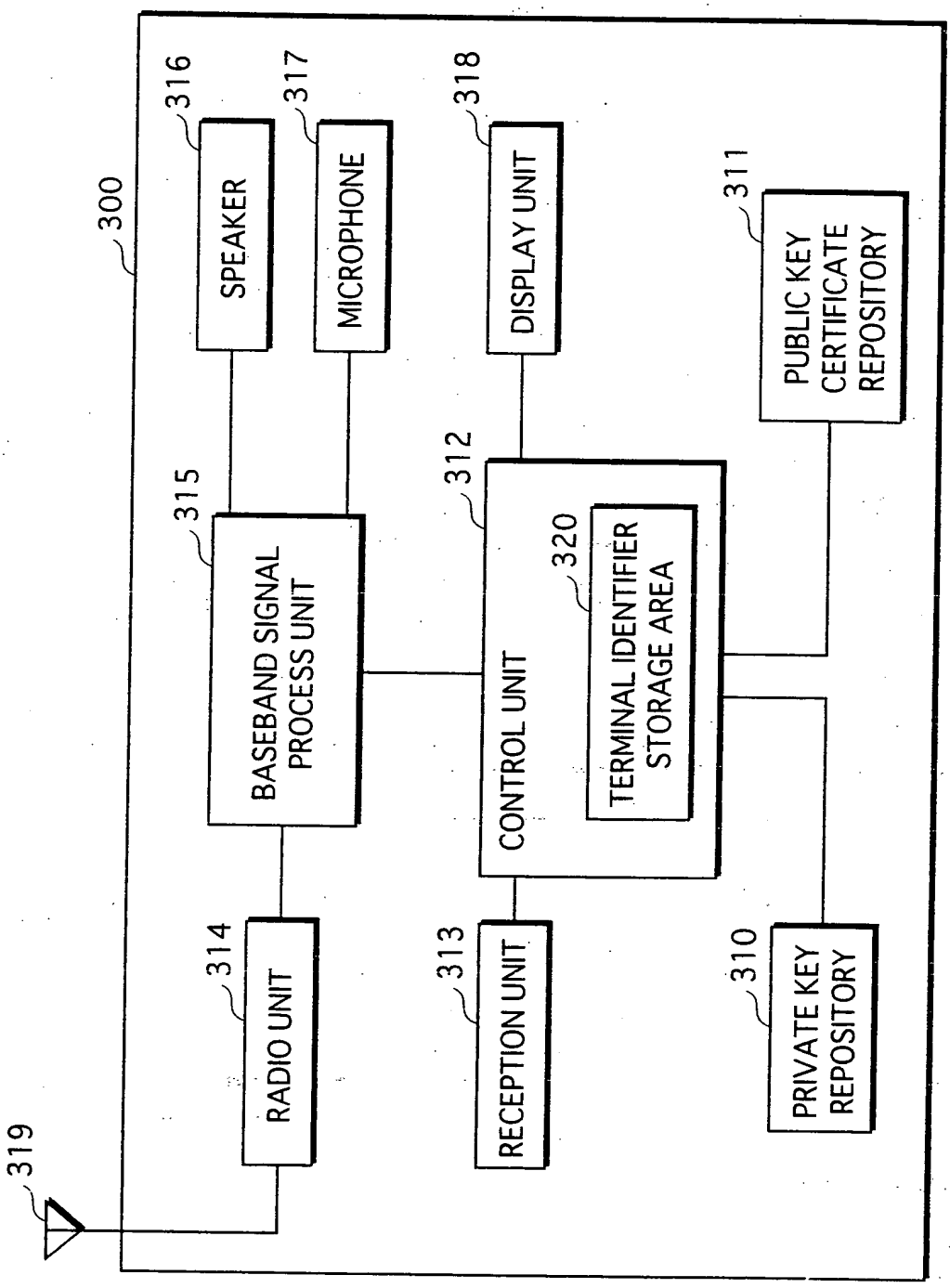

300
316
SPEAKER
317
MICROPHONE
318
DISPLAY UNIT
311
PUBLIC KEY CERTIFICATE REPOSITORY
315
BASEBAND SIGNAL PROCESS UNIT
312
CONTROL UNIT
320
TERMINAL IDENTIFIER STORAGE AREA
314
RADIO UNIT
313
RECEPTION UNIT
310
PRIVATE KEY REPOSITORY
319

FIG.9

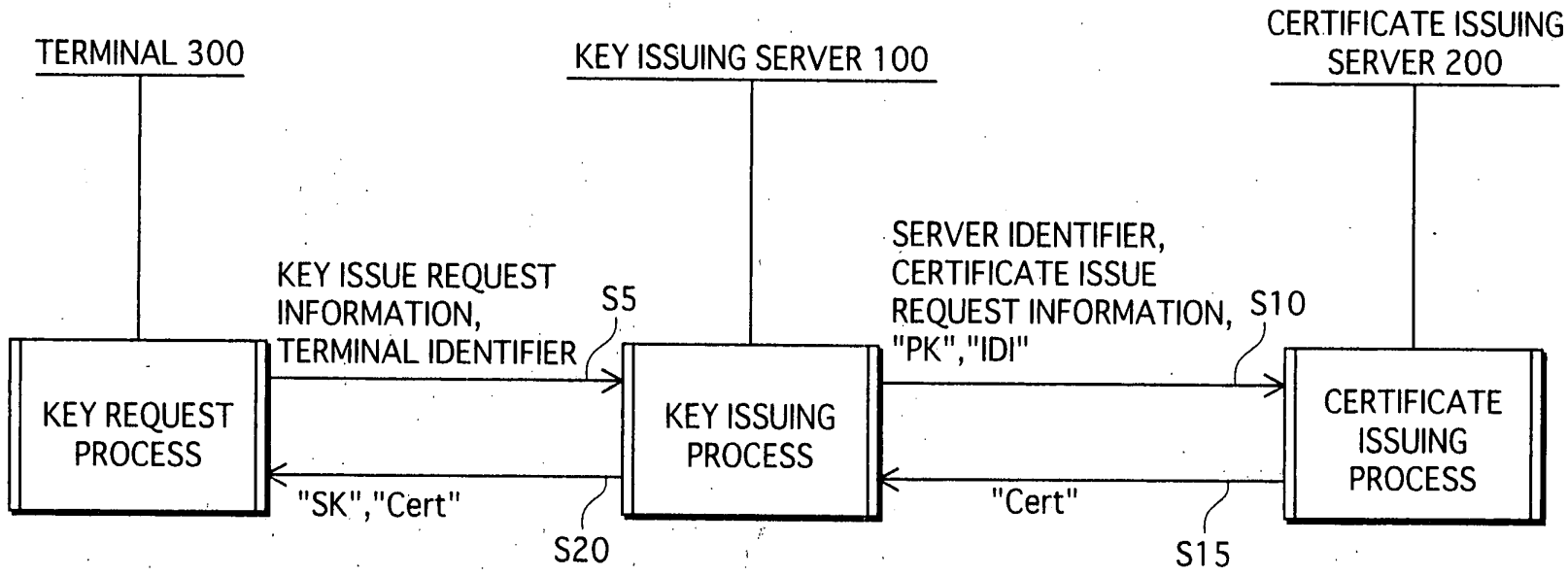

TERMINAL 300
KEY ISSUING SERVER 100
CERTIFICATE ISSUING SERVER 200
KEY REQUEST PROCESS
KEY ISSUING PROCESS
CERTIFICATE ISSUING PROCESS
KEY ISSUE REQUEST INFORMATION, TERMINAL IDENTIFIER
S5
SERVER IDENTIFIER, CERTIFICATE ISSUE REQUEST INFORMATION, "PK","IDI"
S10
"SK","Cert"
S20
"Cert"
S15

FIG.10

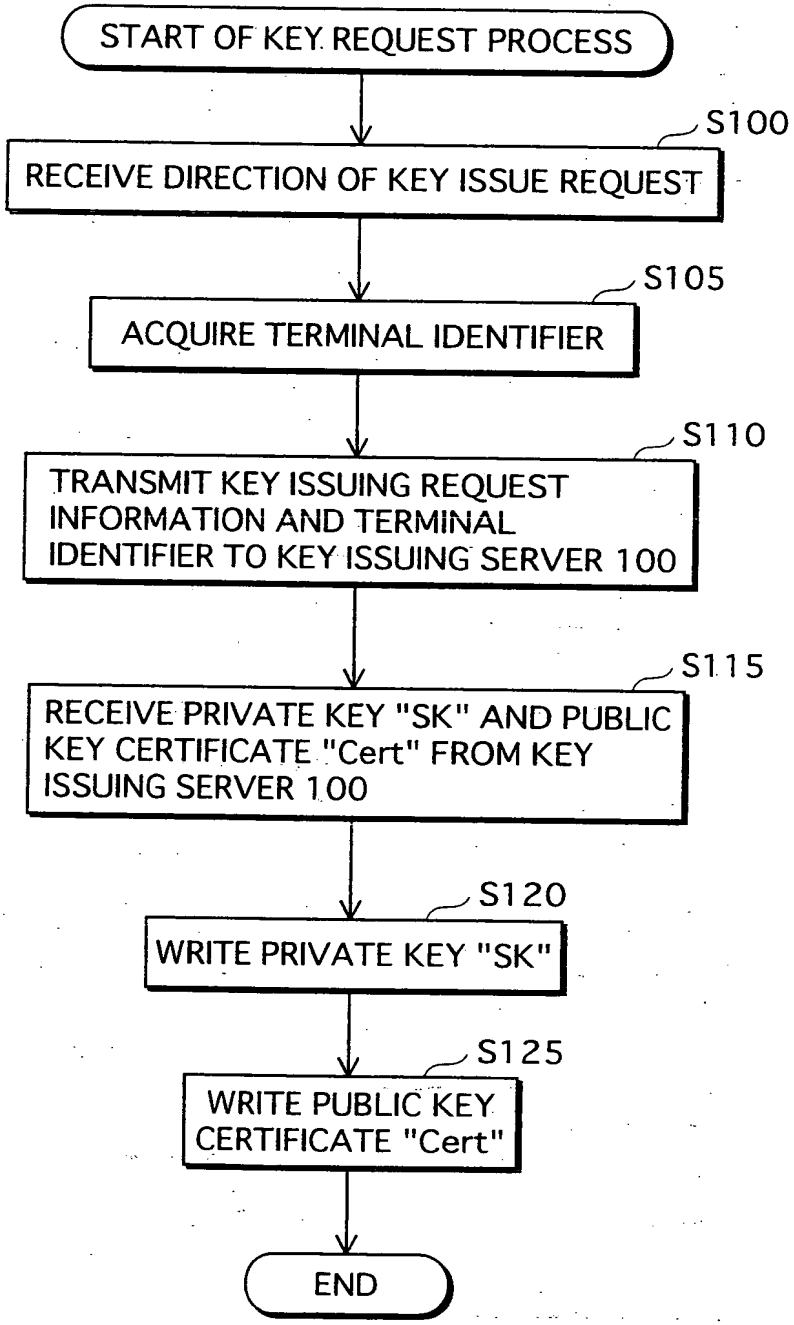

START OF KEY REQUEST PROCESS
S100
RECEIVE DIRECTION OF KEY ISSUE REQUEST
S105
ACQUIRE TERMINAL IDENTIFIER
S110
TRANSMIT KEY ISSUING REQUEST INFORMATION AND TERMINAL IDENTIFIER TO KEY ISSUING SERVER 100
S115
RECEIVE PRIVATE KEY "SK" AND PUBLIC KEY CERTIFICATE "Cert" FROM KEY ISSUING SERVER 100
S120
WRITE PRIVATE KEY "SK"
S125
WRITE PUBLIC KEY CERTIFICATE "Cert"
END

FIG.11

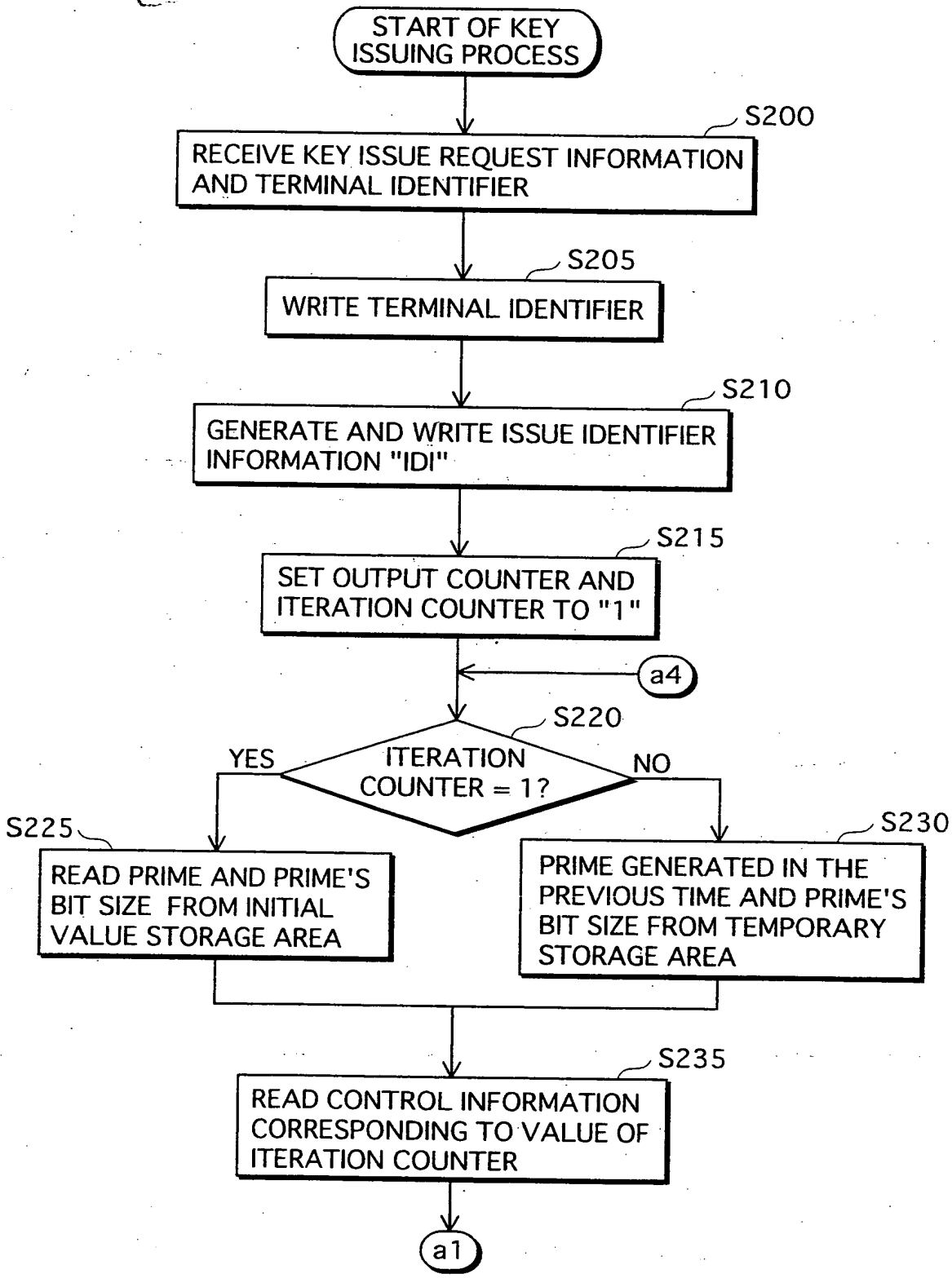

START OF KEY ISSUING PROCESS
S200
RECEIVE KEY ISSUE REQUEST INFORMATION AND TERMINAL IDENTIFIER
S205
WRITE TERMINAL IDENTIFIER
S210
GENERATE AND WRITE ISSUE IDENTIFIER INFORMATION "IDI"
S215
SET OUTPUT COUNTER AND ITERATION COUNTER TO "1"
a4
S220
ITERATION COUNTER = 1?
YES
NO
S225
READ PRIME AND PRIME'S BIT SIZE FROM INITIAL VALUE STORAGE AREA
S230
PRIME GENERATED IN THE PREVIOUS TIME AND PRIME'S BIT SIZE FROM TEMPORARY STORAGE AREA
S235
READ CONTROL INFORMATION CORRESPONDING TO VALUE OF ITERATION COUNTER
a1

FIG.12

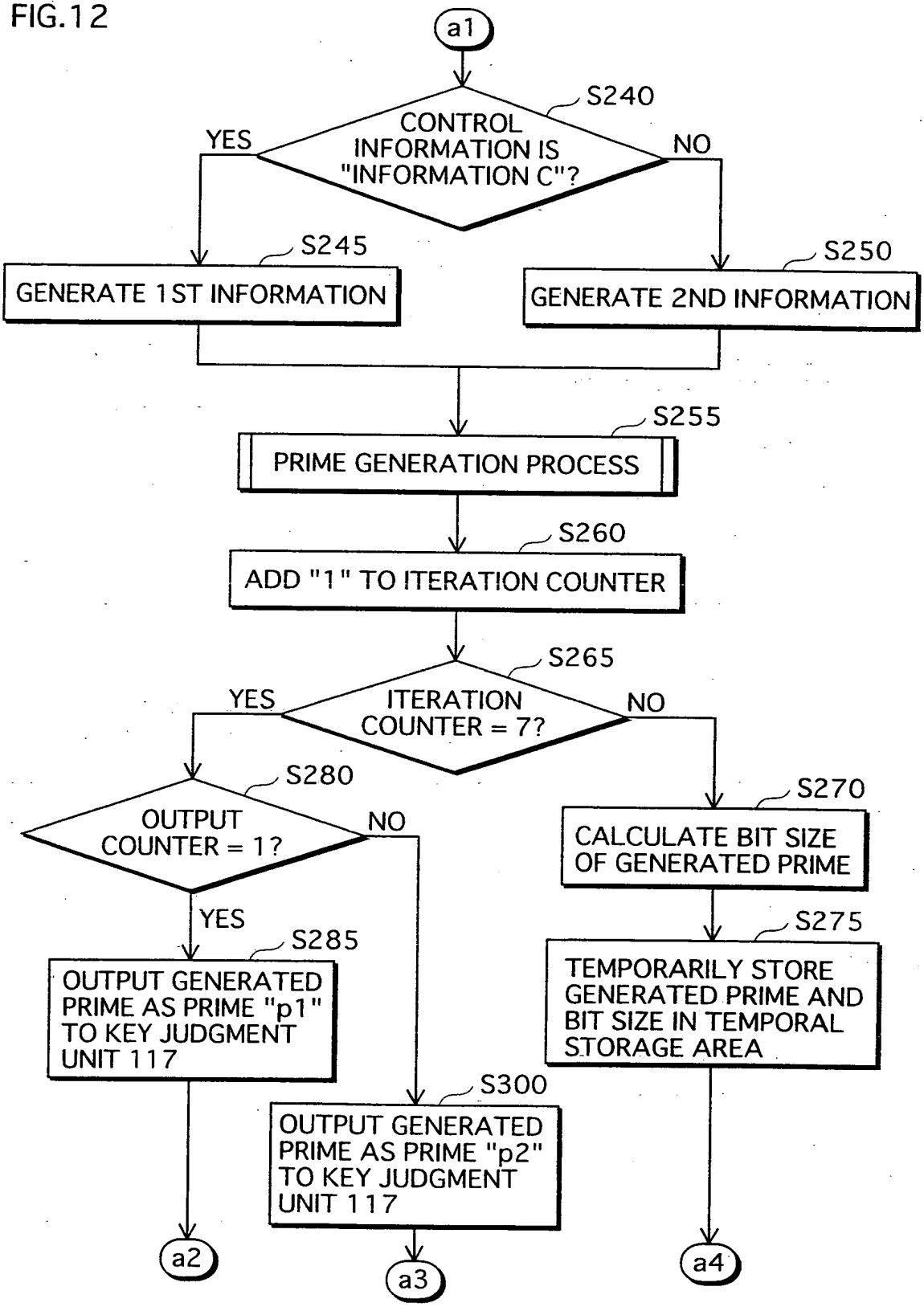

a1
S240
CONTROL INFORMATION IS "INFORMATION C"?
YES
NO
S245
GENERATE 1ST INFORMATION
S250
GENERATE 2ND INFORMATION
S255
PRIME GENERATION PROCESS
S260
ADD "1" TO ITERATION COUNTER
S265
ITERATION COUNTER = 7?
YES
NO
S280
OUTPUT COUNTER = 1?
NO
YES
S285
OUTPUT GENERATED PRIME AS PRIME "p1" TO KEY JUDGMENT UNIT 117
S270
CALCULATE BIT SIZE OF GENERATED PRIME
S275
TEMPORARILY STORE GENERATED PRIME AND BIT SIZE IN TEMPORAL STORAGE AREA
S300
OUTPUT GENERATED PRIME AS PRIME "p2" TO KEY JUDGMENT UNIT 117
a2
a3
a4

FIG.13

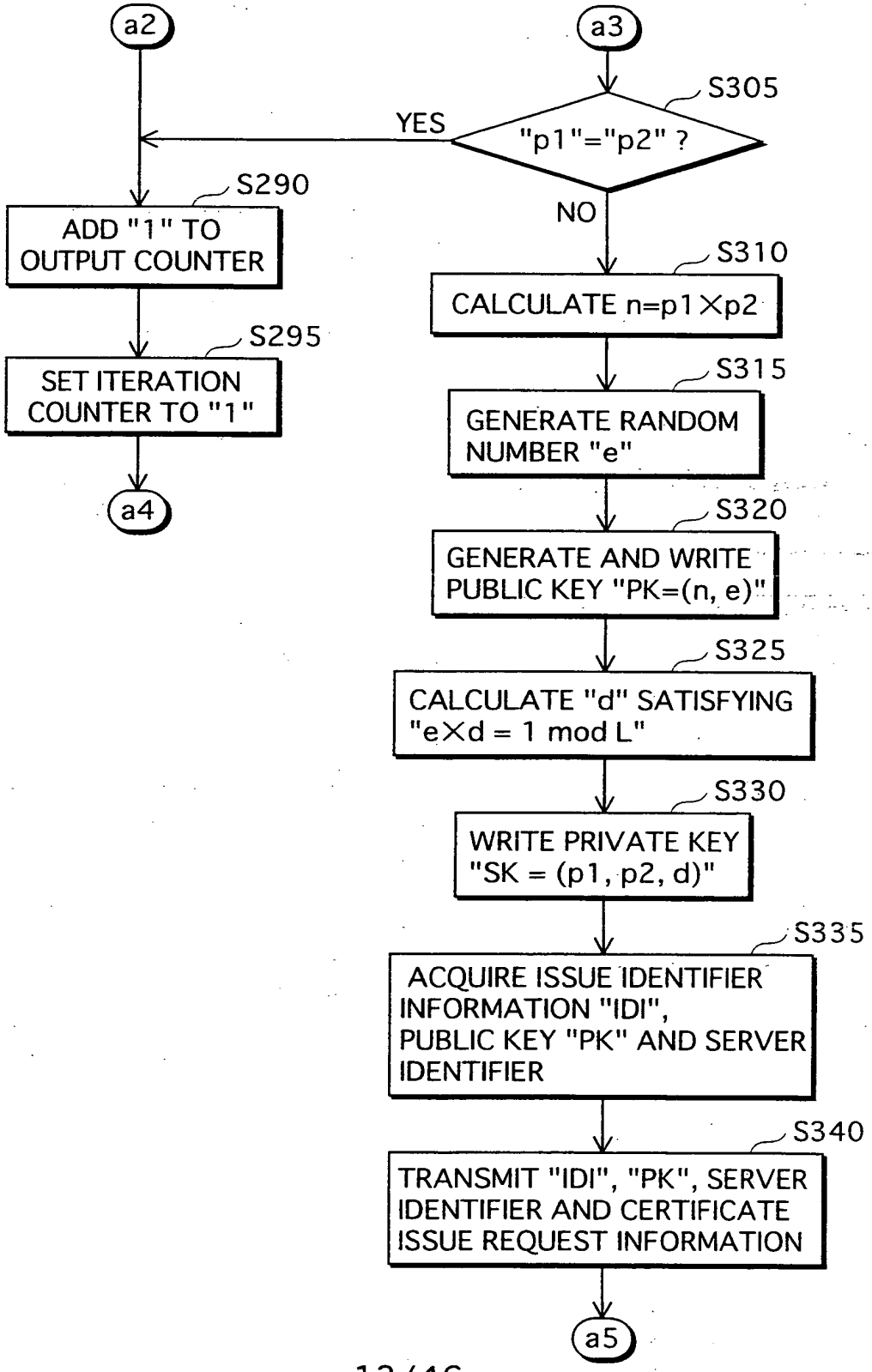

a2
a3
S305
"p1"="p2" ?
YES
NO
S290
ADD "1" TO OUTPUT COUNTER
S295
SET ITERATION COUNTER TO "1"
a4
S310
CALCULATE n=p1×p2
S315
GENERATE RANDOM NUMBER "e"
S320
GENERATE AND WRITE PUBLIC KEY "PK=(n, e)"
S325
CALCULATE "d" SATISFYING "e×d = 1 mod L"
S330
WRITE PRIVATE KEY "SK = (p1, p2, d)"
S335
ACQUIRE ISSUE IDENTIFIER INFORMATION "IDI", PUBLIC KEY "PK" AND SERVER IDENTIFIER
S340
TRANSMIT "IDI", "PK", SERVER IDENTIFIER AND CERTIFICATE ISSUE REQUEST INFORMATION
a5

FIG.14

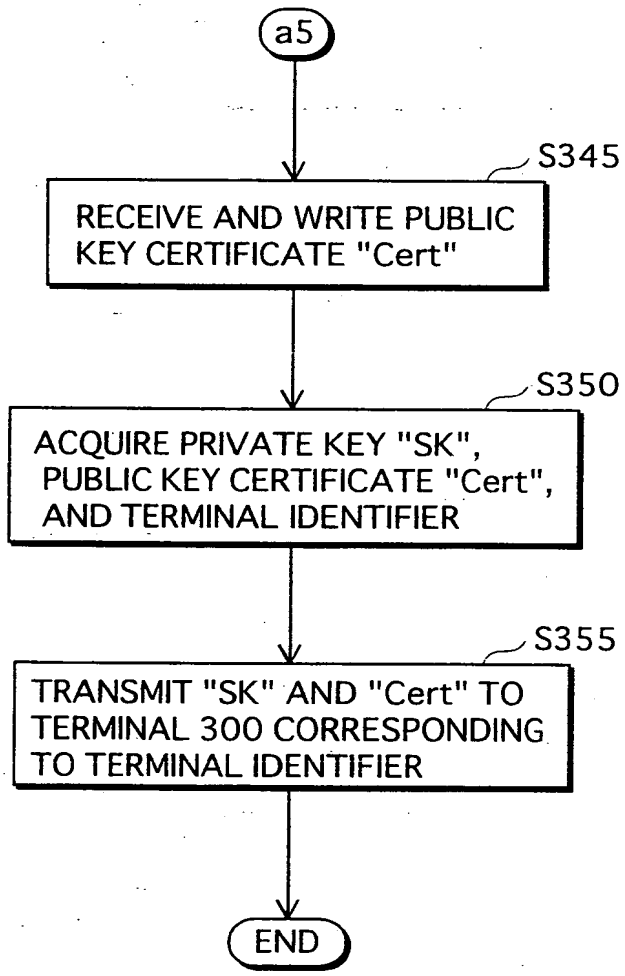

a5
S345
RECEIVE AND WRITE PUBLIC KEY CERTIFICATE "Cert"
S350
ACQUIRE PRIVATE KEY "SK", PUBLIC KEY CERTIFICATE "Cert", AND TERMINAL IDENTIFIER
S355
TRANSMIT "SK" AND "Cert" TO TERMINAL 300 CORRESPONDING TO TERMINAL IDENTIFIER
END

FIG.15

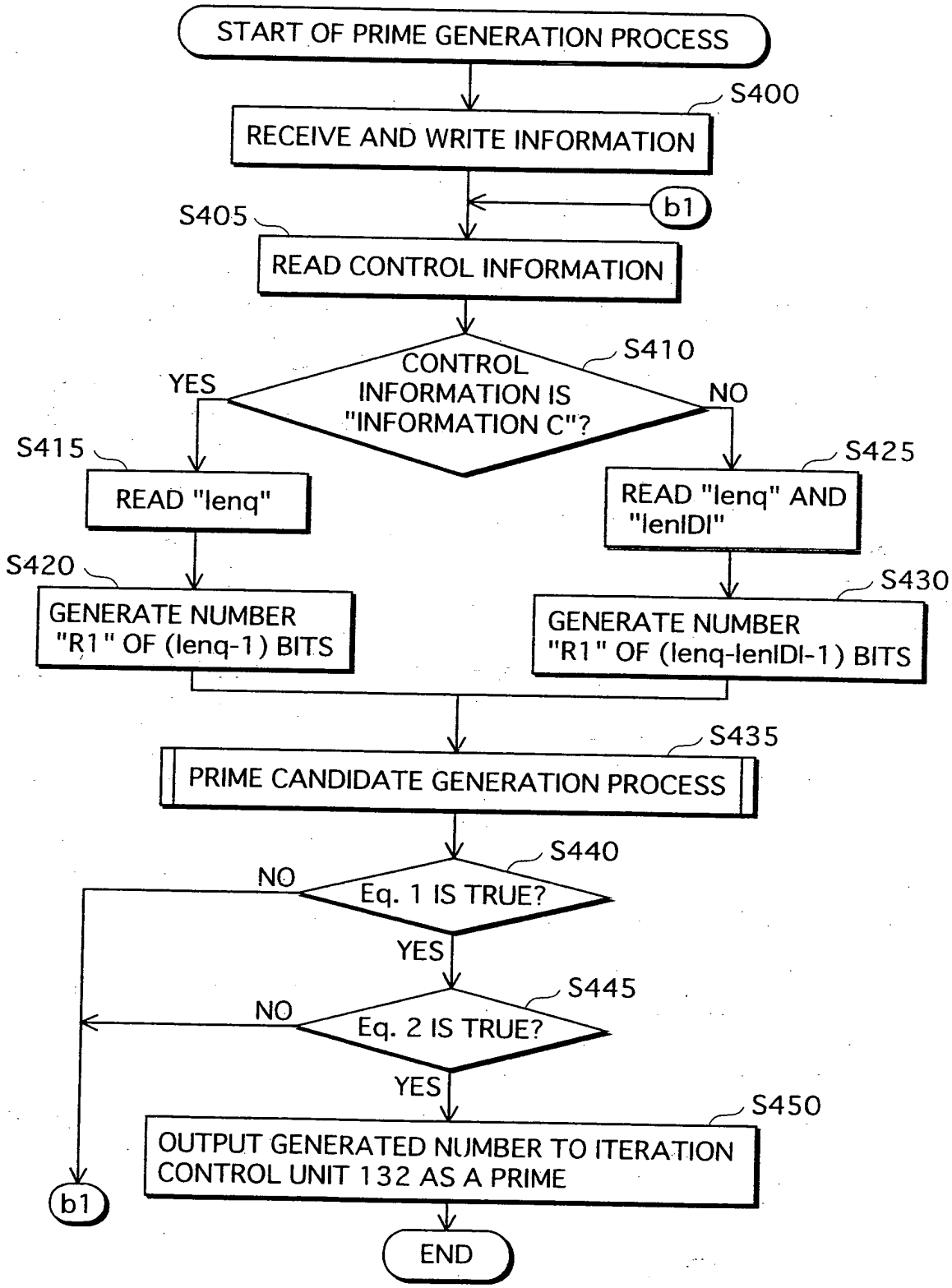

START OF PRIME GENERATION PROCESS
S400
RECEIVE AND WRITE INFORMATION
b1
S405
READ CONTROL INFORMATION
S410
CONTROL INFORMATION IS "INFORMATION C"?
YES
NO
S415
READ "lenq"
S425
READ "lenq" AND "lenIDI"
S420
GENERATE NUMBER "R1" OF (lenq-1) BITS
S430
GENERATE NUMBER "R1" OF (lenq-lenIDI-1) BITS
S435
PRIME CANDIDATE GENERATION PROCESS
S440
Eq. 1 IS TRUE?
NO
YES
S445
Eq. 2 IS TRUE?
NO
YES
S450
OUTPUT GENERATED NUMBER TO ITERATION CONTROL UNIT 132 AS A PRIME
b1
END

FIG.16

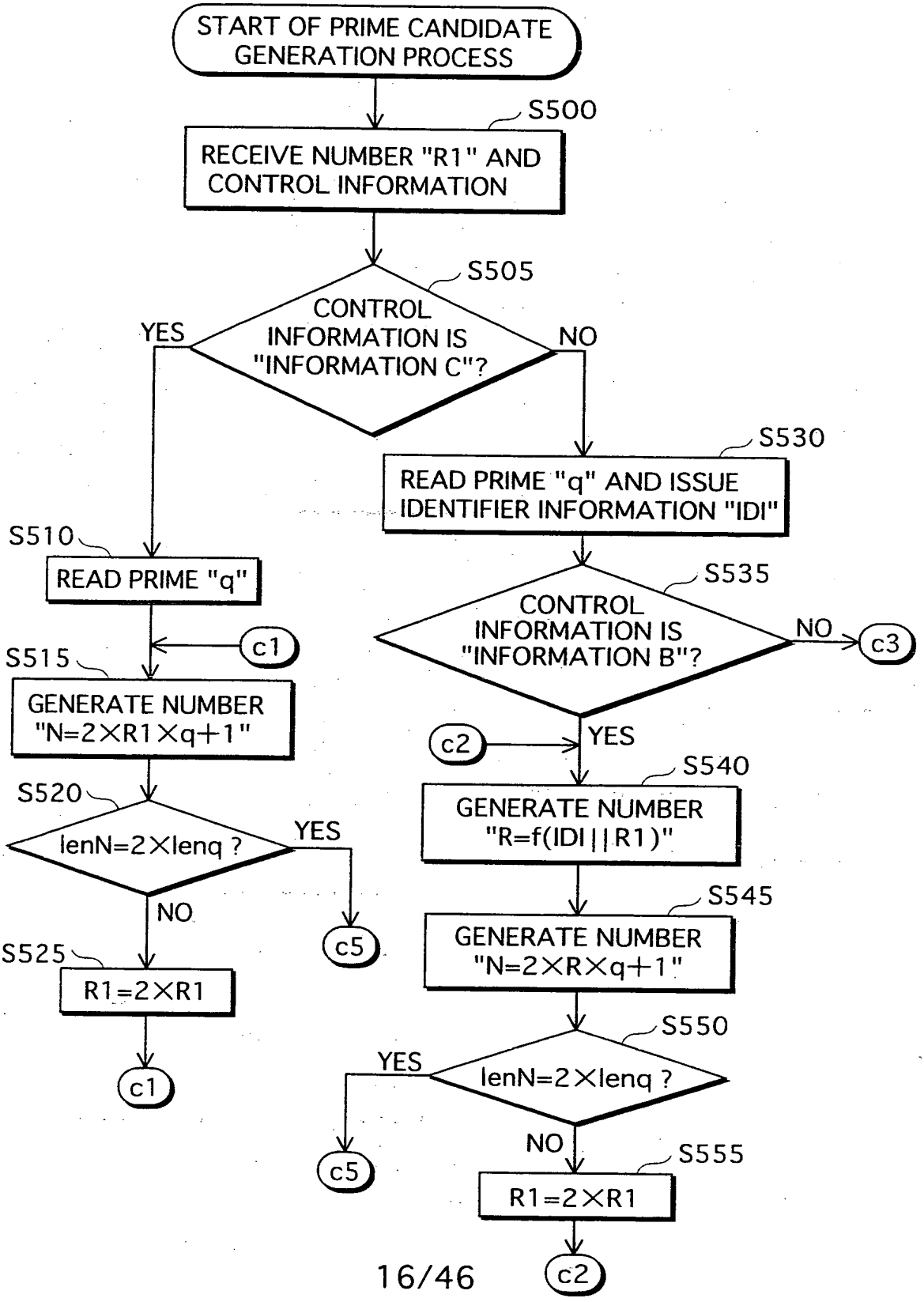

START OF PRIME CANDIDATE GENERATION PROCESS
S500
RECEIVE NUMBER "R1" AND CONTROL INFORMATION
S505
CONTROL INFORMATION IS "INFORMATION C"?
YES
NO
S510
READ PRIME "q"
c1
S515
GENERATE NUMBER "N=2×R1×q+1"
S520
lenN=2×lenq ?
YES
NO
c5
S525
R1=2×R1
c1
S530
READ PRIME "q" AND ISSUE IDENTIFIER INFORMATION "IDI"
S535
CONTROL INFORMATION IS "INFORMATION B"?
NO
c3
c2
YES
S540
GENERATE NUMBER "R=f(IDI||R1)"
S545
GENERATE NUMBER "N=2×R×q+1"
S550
lenN=2×lenq ?
YES
c5
NO
S555
R1=2×R1
c2

FIG.17

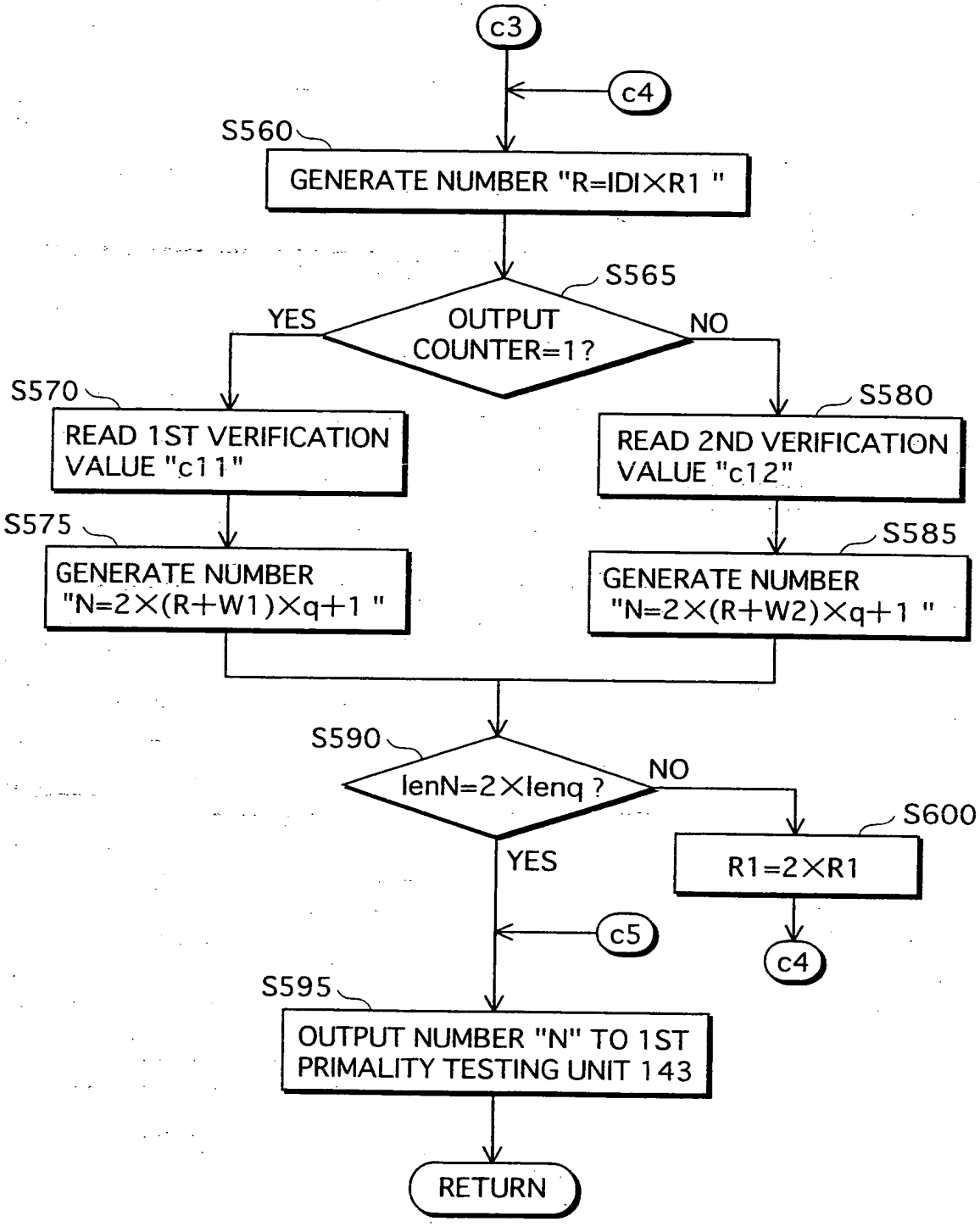

c3
c4
S560
GENERATE NUMBER "R=IDI×R1 "
S565
OUTPUT COUNTER=1?
YES
NO
S570
READ 1ST VERIFICATION VALUE "c11"
S580
READ 2ND VERIFICATION VALUE "c12"
S575
GENERATE NUMBER "N=2×(R+W1)×q+1 "
S585
GENERATE NUMBER "N=2×(R+W2)×q+1 "
S590
lenN=2×lenq ?
NO
S600
R1=2×R1
YES
c5
c4
S595
OUTPUT NUMBER "N" TO 1ST PRIMALITY TESTING UNIT 143
RETURN

FIG.18

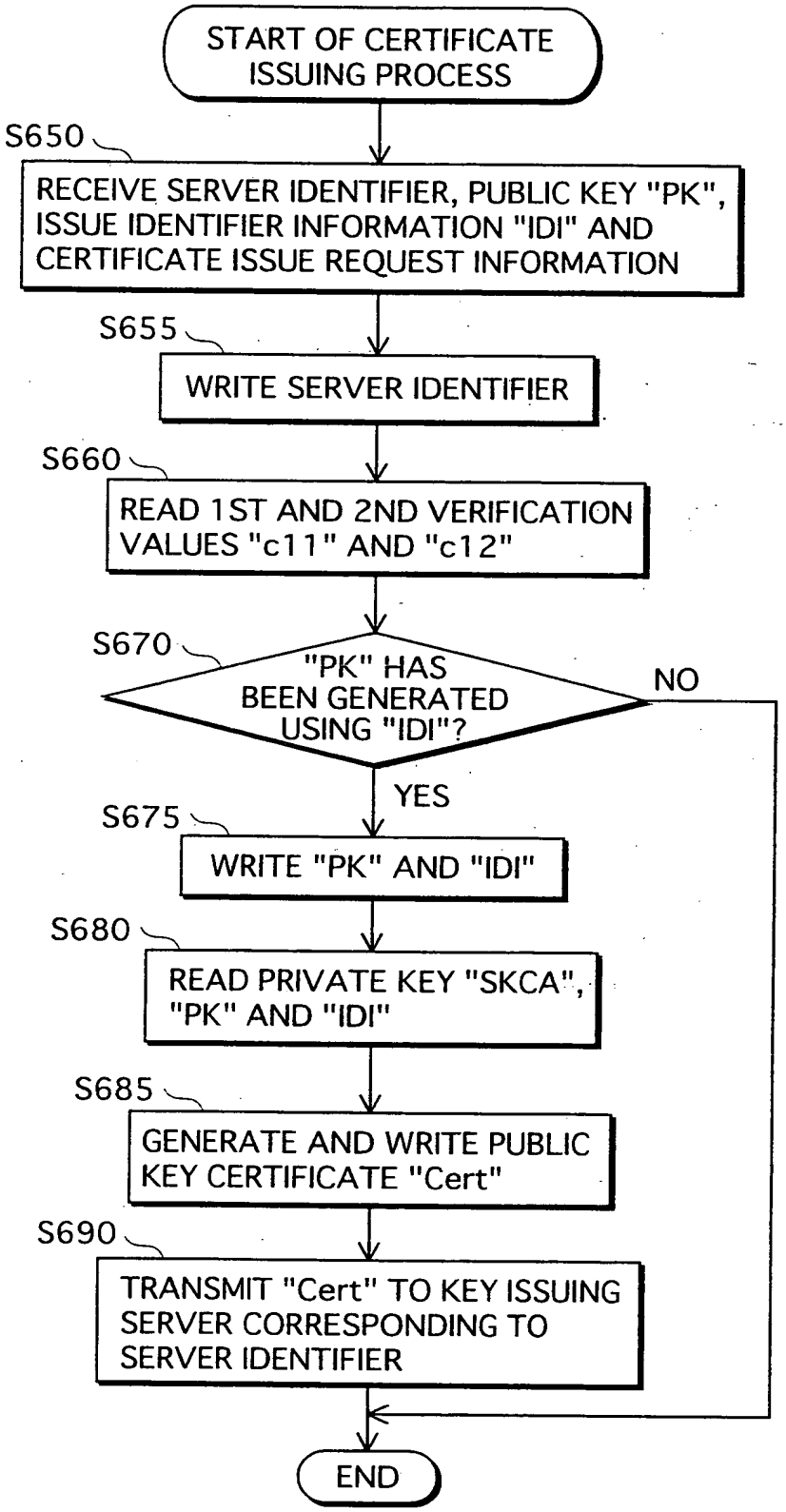

START OF CERTIFICATE ISSUING PROCESS
S650
RECEIVE SERVER IDENTIFIER, PUBLIC KEY "PK", ISSUE IDENTIFIER INFORMATION "IDI" AND CERTIFICATE ISSUE REQUEST INFORMATION
S655
WRITE SERVER IDENTIFIER
S660
READ 1ST AND 2ND VERIFICATION VALUES "c11" AND "c12"
S670
"PK" HAS BEEN GENERATED USING "IDI"?
NO
YES
S675
WRITE "PK" AND "IDI"
S680
READ PRIVATE KEY "SKCA", "PK" AND "IDI"
S685
GENERATE AND WRITE PUBLIC KEY CERTIFICATE "Cert"
S690
TRANSMIT "Cert" TO KEY ISSUING SERVER CORRESPONDING TO SERVER IDENTIFIER
END

FIG.19

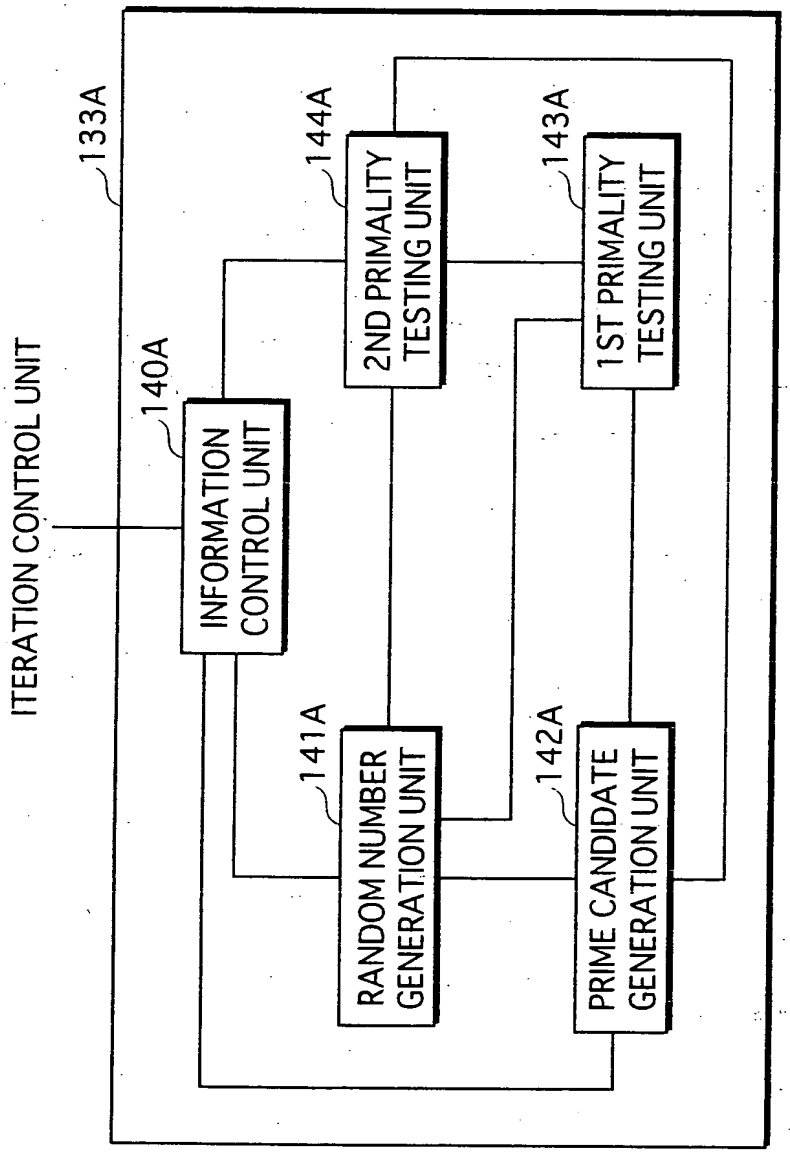

133A
ITERATION CONTROL UNIT
140A
INFORMATION CONTROL UNIT
144A
2ND PRIMALITY TESTING UNIT
143A
1ST PRIMALITY TESTING UNIT
141A
RANDOM NUMBER GENERATION UNIT
142A
PRIME CANDIDATE GENERATION UNIT

FIG.20

T250

SERVER IDENTIFIER	VERIFICATION VALUE
SID A	c1
SID B	c2
SID C	c3

FIG.21

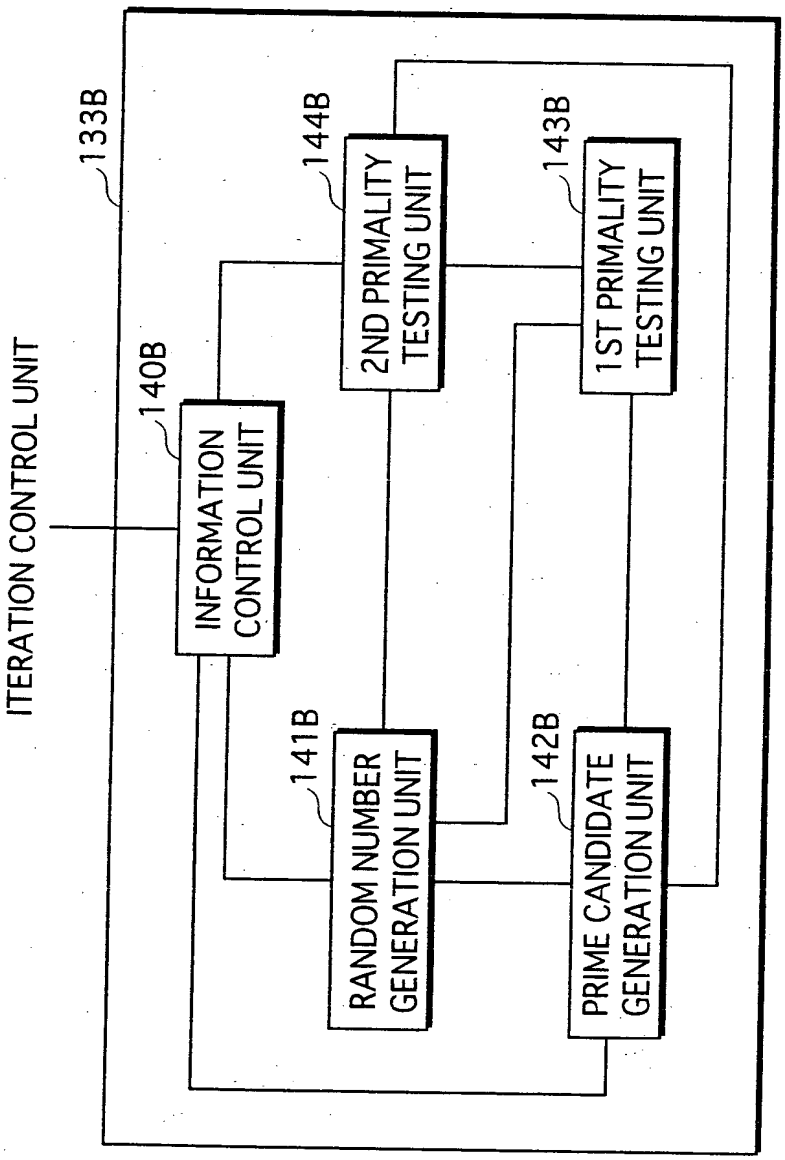

ITERATION CONTROL UNIT
133B
140B
INFORMATION CONTROL UNIT
144B
2ND PRIMALITY TESTING UNIT
143B
1ST PRIMALITY TESTING UNIT
141B
RANDOM NUMBER GENERATION UNIT
142B
PRIME CANDIDATE GENERATION UNIT

FIG.22

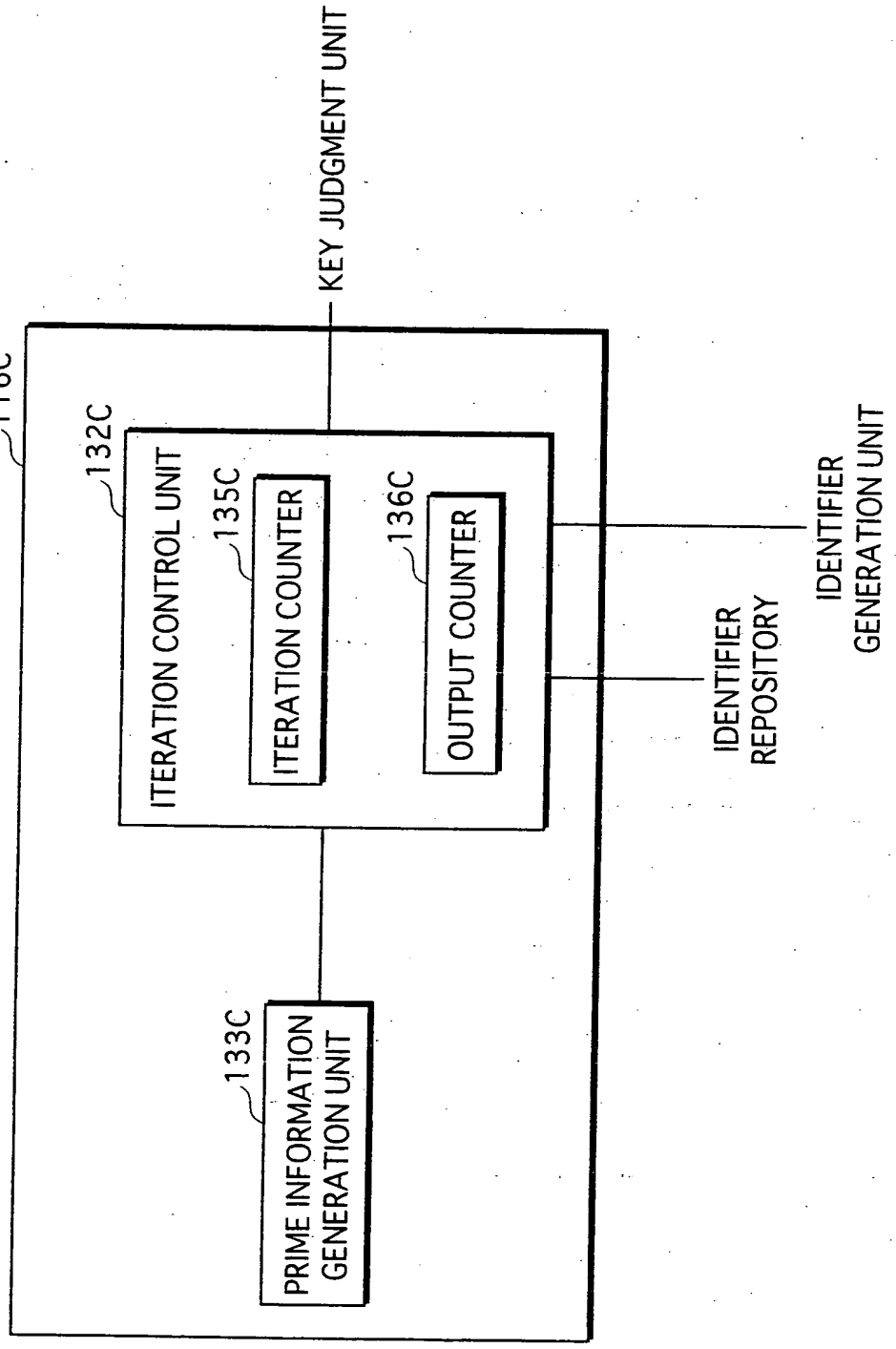

KEY JUDGMENT UNIT
116C
132C
ITERATION CONTROL UNIT
135C
ITERATION COUNTER
136C
OUTPUT COUNTER
133C
PRIME INFORMATION GENERATION UNIT
IDENTIFIER REPOSITORY
IDENTIFIER GENERATION UNIT

FIG.23

T150

NUMBER OF ITERATIONS	CONTROL INFORMATION
1	INFORMATION C
2	INFORMATION C
3	INFORMATION C
4	INFORMATION C
5	INFORMATION C
6	INFORMATION AB

FIG.24

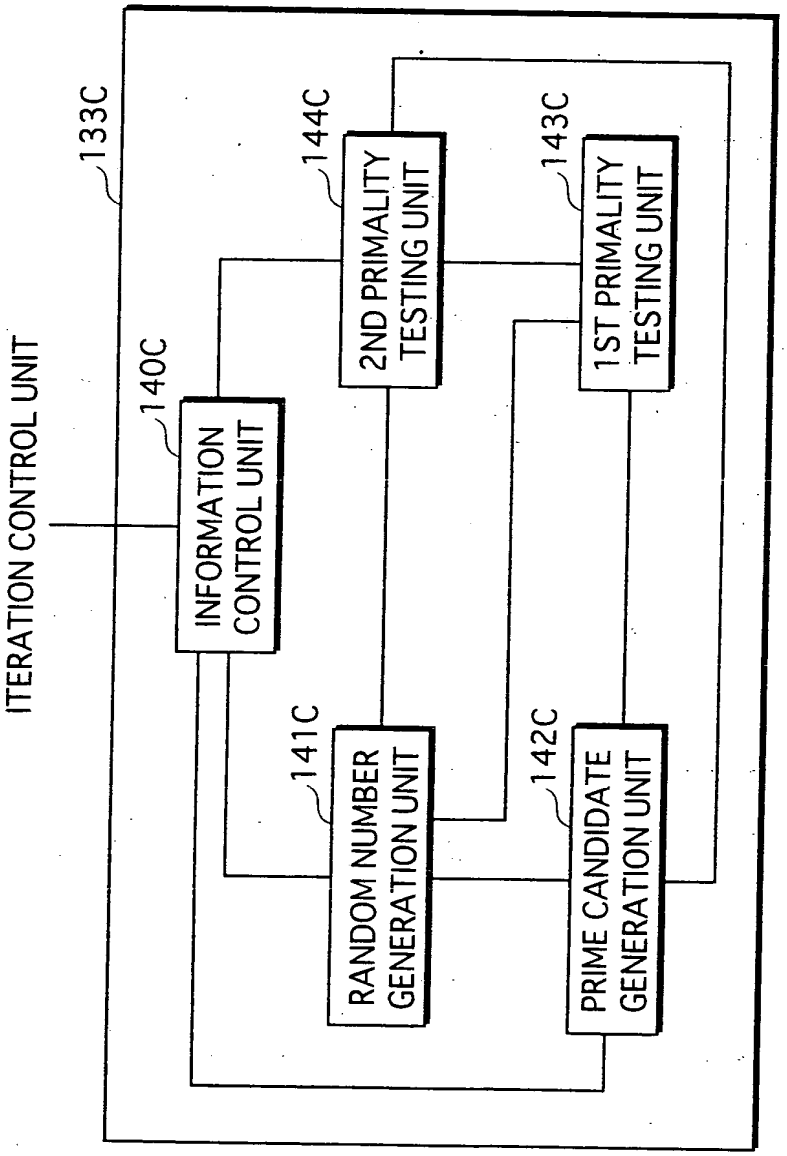

ITERATION CONTROL UNIT
133C
140C
INFORMATION CONTROL UNIT
144C
2ND PRIMALITY TESTING UNIT
143C
1ST PRIMALITY TESTING UNIT
141C
RANDOM NUMBER GENERATION UNIT
142C
PRIME CANDIDATE GENERATION UNIT

FIG.25

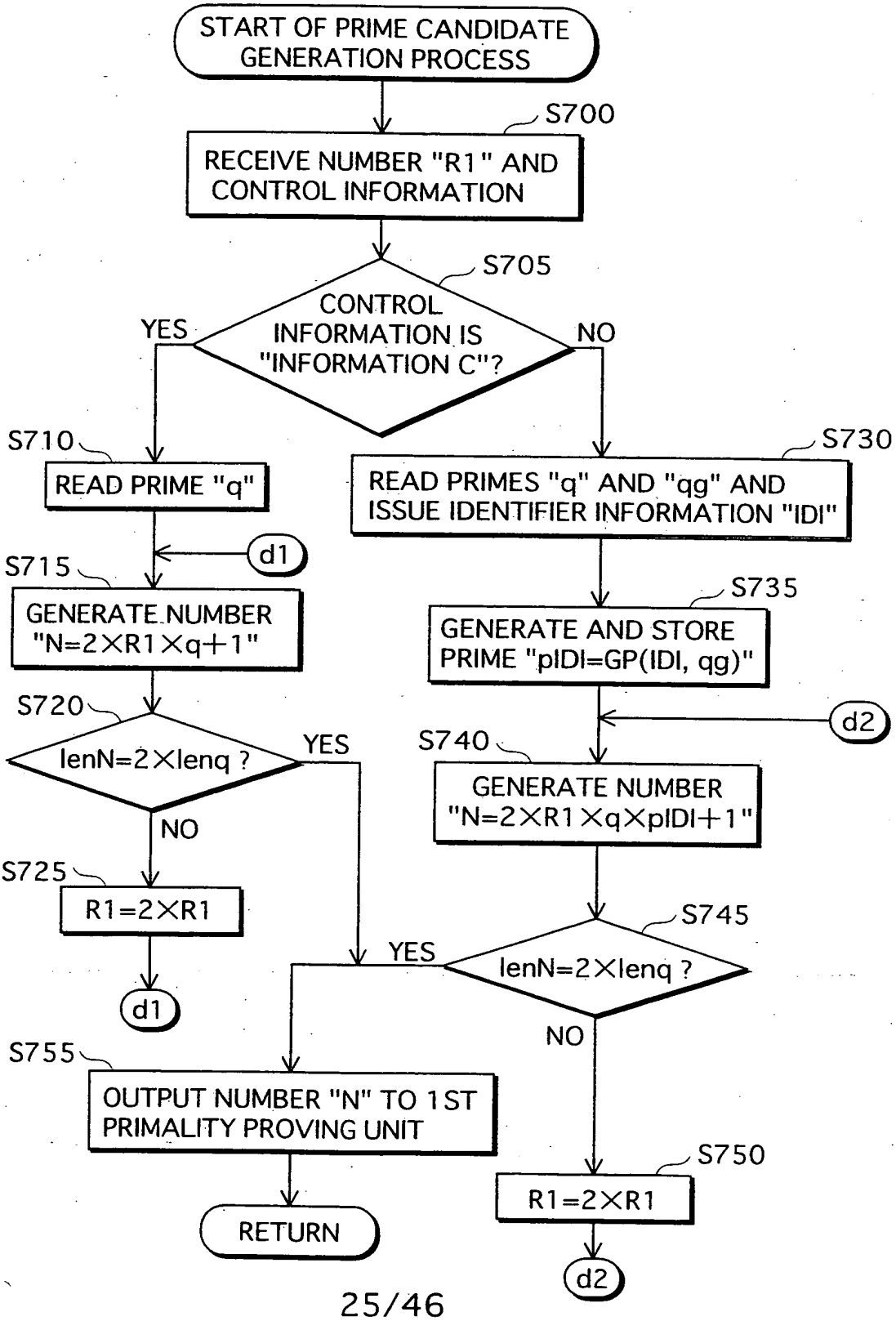

START OF PRIME CANDIDATE GENERATION PROCESS
S700
RECEIVE NUMBER "R1" AND CONTROL INFORMATION
S705
CONTROL INFORMATION IS "INFORMATION C"?
YES
NO
S710
READ PRIME "q"
S730
READ PRIMES "q" AND "qg" AND ISSUE IDENTIFIER INFORMATION "IDI"
d1
S715
GENERATE NUMBER "N=2×R1×q+1"
S735
GENERATE AND STORE PRIME "pIDI=GP(IDI, qg)"
d2
S720
lenN=2×lenq ?
YES
NO
S740
GENERATE NUMBER "N=2×R1×q×pIDI+1"
S725
R1=2×R1
S745
lenN=2×lenq ?
YES
NO
d1
S755
OUTPUT NUMBER "N" TO 1ST PRIMALITY PROVING UNIT
S750
R1=2×R1
RETURN
d2

FIG.26

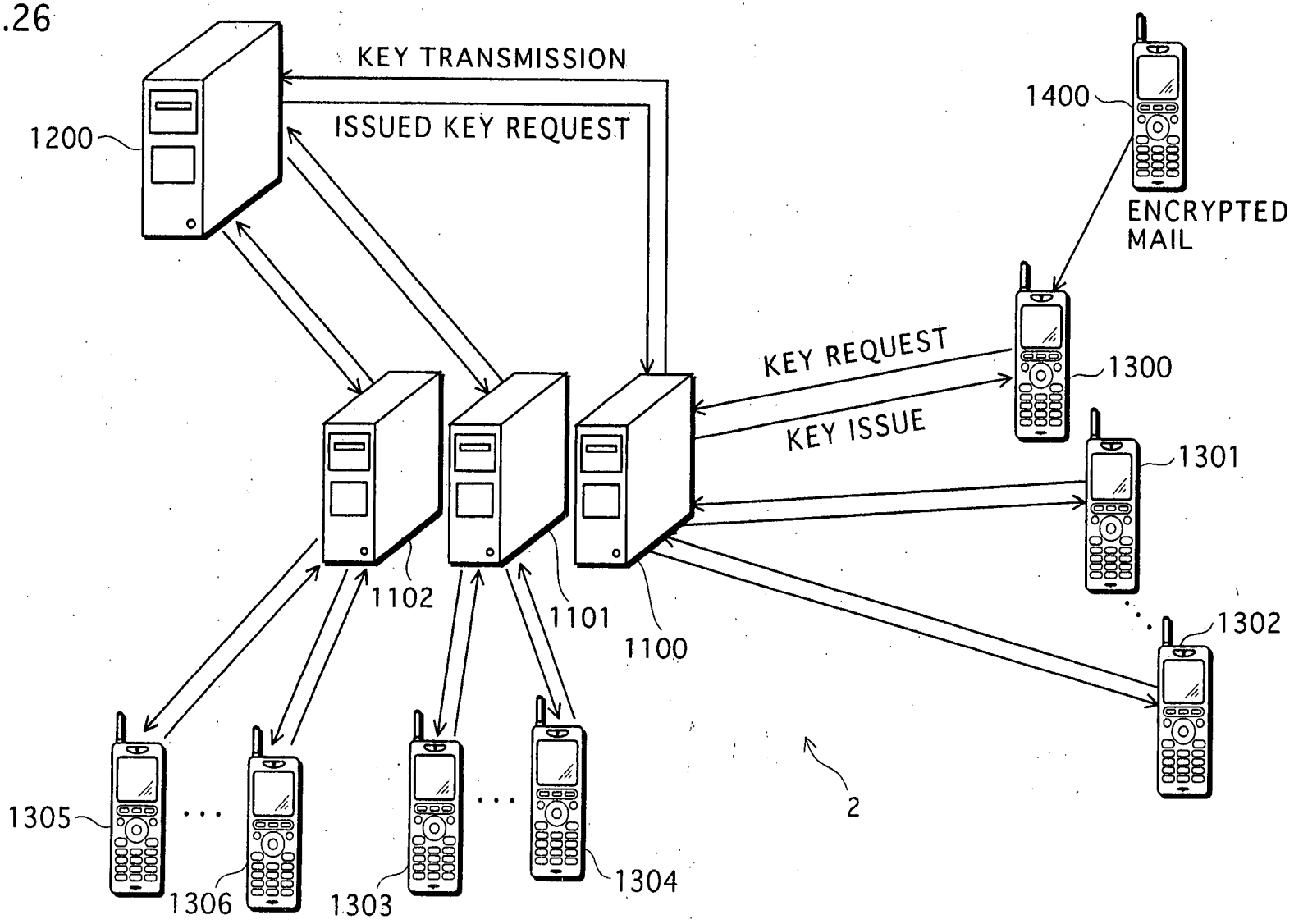

KEY TRANSMISSION
ISSUED KEY REQUEST
1200
1400
ENCRYPTED MAIL
KEY REQUEST
KEY ISSUE
1300
1301
1302
1102
1101
1100
1305
1306
1303
1304
2

FIG.27

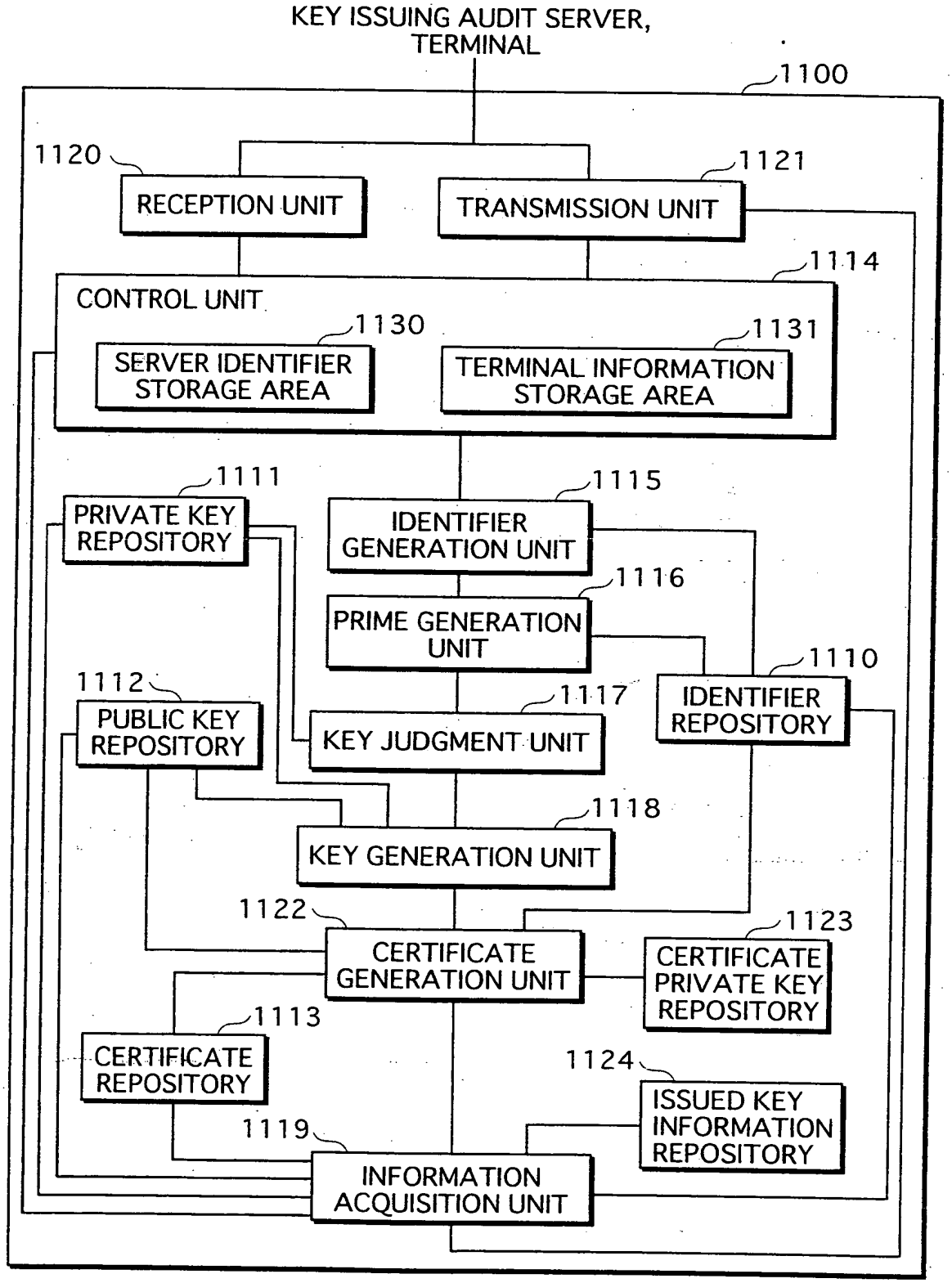

KEY ISSUING AUDIT SERVER, TERMINAL
1100
1120
RECEPTION UNIT
1121
TRANSMISSION UNIT
1114
CONTROL UNIT
1130
SERVER IDENTIFIER STORAGE AREA
1131
TERMINAL INFORMATION STORAGE AREA
1111
PRIVATE KEY REPOSITORY
1115
IDENTIFIER GENERATION UNIT
1116
PRIME GENERATION UNIT
1110
IDENTIFIER REPOSITORY
1112
PUBLIC KEY REPOSITORY
1117
KEY JUDGMENT UNIT
1118
KEY GENERATION UNIT
1122
CERTIFICATE GENERATION UNIT
1123
CERTIFICATE PRIVATE KEY REPOSITORY
1113
CERTIFICATE REPOSITORY
1124
ISSUED KEY INFORMATION REPOSITORY
1119
INFORMATION ACQUISITION UNIT

FIG.28

T1100

ISSUED PUBLIC KEY	ISSUED IDENTIFIER INFORMATION
PK 1	IDI1
PK 2	IDI 2
⋮	⋮
PK	IDI

FIG.29

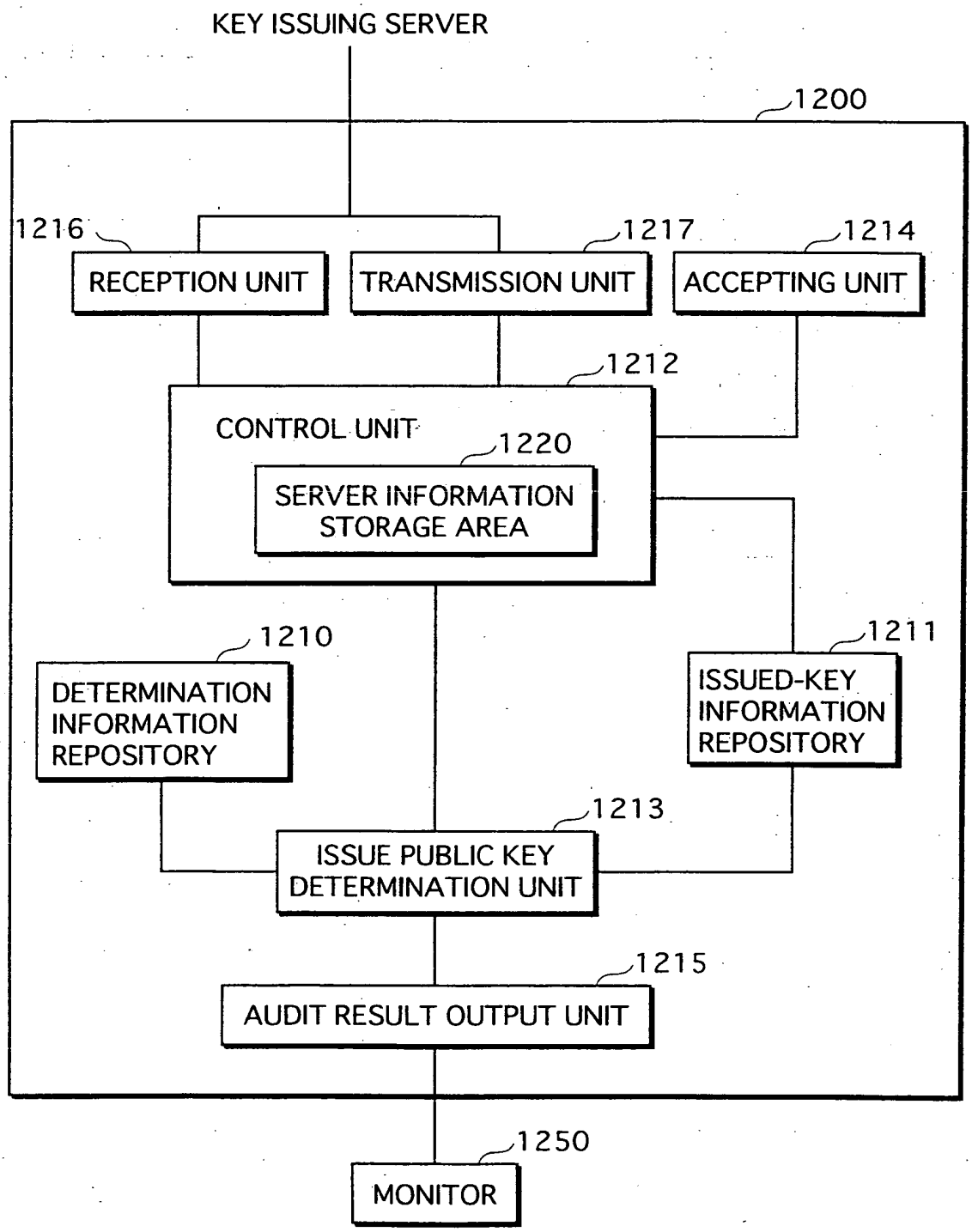

KEY ISSUING SERVER
1200
1216
1217
1214
RECEPTION UNIT
TRANSMISSION UNIT
ACCEPTING UNIT
1212
CONTROL UNIT
1220
SERVER INFORMATION STORAGE AREA
1210
DETERMINATION INFORMATION REPOSITORY
1211
ISSUED-KEY INFORMATION REPOSITORY
1213
ISSUE PUBLIC KEY DETERMINATION UNIT
1215
AUDIT RESULT OUTPUT UNIT
1250
MONITOR

FIG.30

T1200

SERVER IDENTIFIER	1ST VERIFICATION VALUE	2ND VERIFICATION VALUE
SID A	c11	c12
SID B	c21	c22
SID C	c31	c33

FIG.31

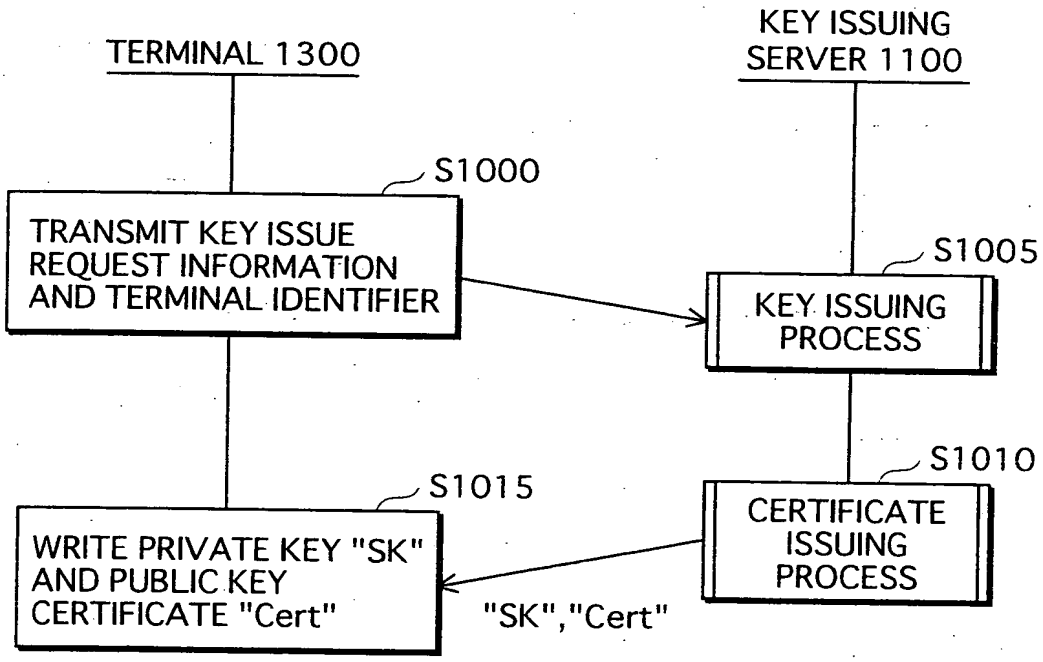

TERMINAL 1300
KEY ISSUING SERVER 1100
S1000
TRANSMIT KEY ISSUE REQUEST INFORMATION AND TERMINAL IDENTIFIER
S1005
KEY ISSUING PROCESS
S1010
CERTIFICATE ISSUING PROCESS
S1015
WRITE PRIVATE KEY "SK" AND PUBLIC KEY CERTIFICATE "Cert"
"SK","Cert"

FIG.32

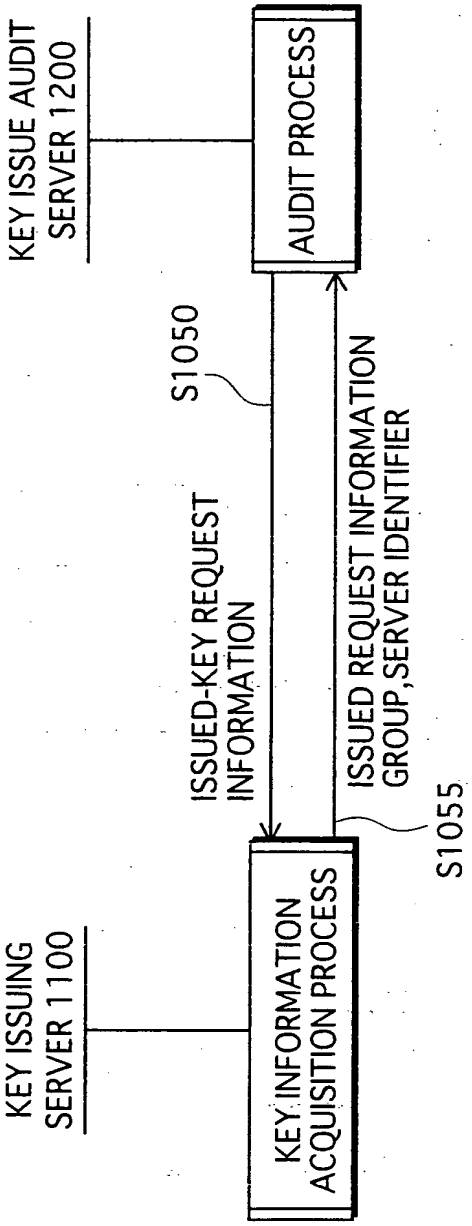

KEY ISSUE AUDIT SERVER 1200
AUDIT PROCESS
S1050
ISSUED-KEY REQUEST INFORMATION
ISSUED REQUEST INFORMATION GROUP, SERVER IDENTIFIER
S1055
KEY ISSUING SERVER 1100
KEY INFORMATION ACQUISITION PROCESS

FIG.33

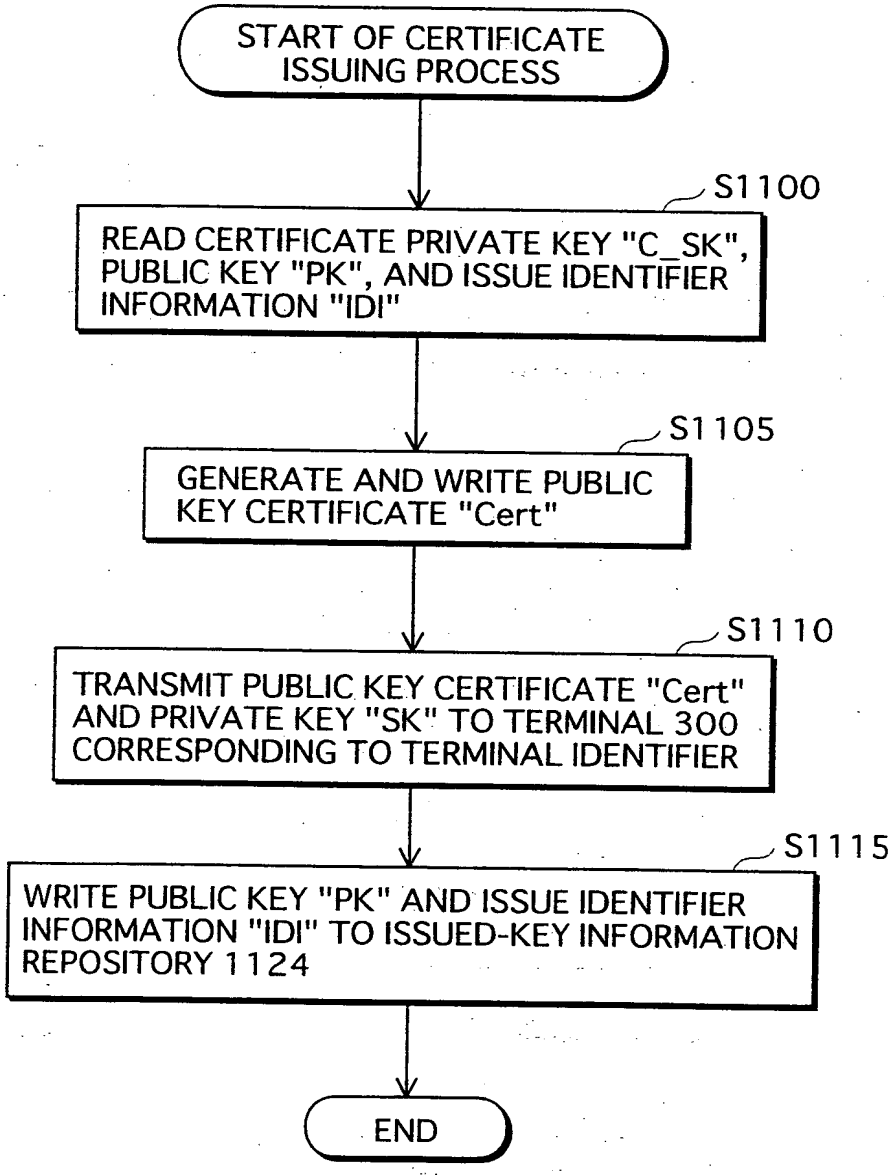

START OF CERTIFICATE ISSUING PROCESS
S1100
READ CERTIFICATE PRIVATE KEY "C_SK", PUBLIC KEY "PK", AND ISSUE IDENTIFIER INFORMATION "IDI"
S1105
GENERATE AND WRITE PUBLIC KEY CERTIFICATE "Cert"
S1110
TRANSMIT PUBLIC KEY CERTIFICATE "Cert" AND PRIVATE KEY "SK" TO TERMINAL 300 CORRESPONDING TO TERMINAL IDENTIFIER
S1115
WRITE PUBLIC KEY "PK" AND ISSUE IDENTIFIER INFORMATION "IDI" TO ISSUED-KEY INFORMATION REPOSITORY 1124
END

FIG.34

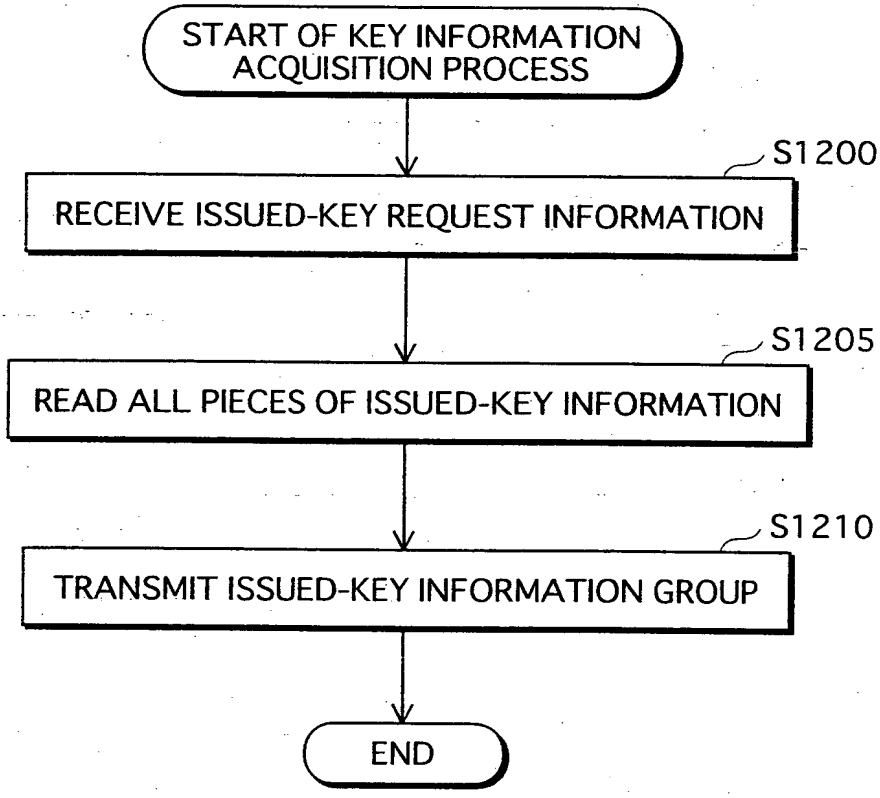

START OF KEY INFORMATION ACQUISITION PROCESS
S1200
RECEIVE ISSUED-KEY REQUEST INFORMATION
S1205
READ ALL PIECES OF ISSUED-KEY INFORMATION
S1210
TRANSMIT ISSUED-KEY INFORMATION GROUP
END

FIG.35

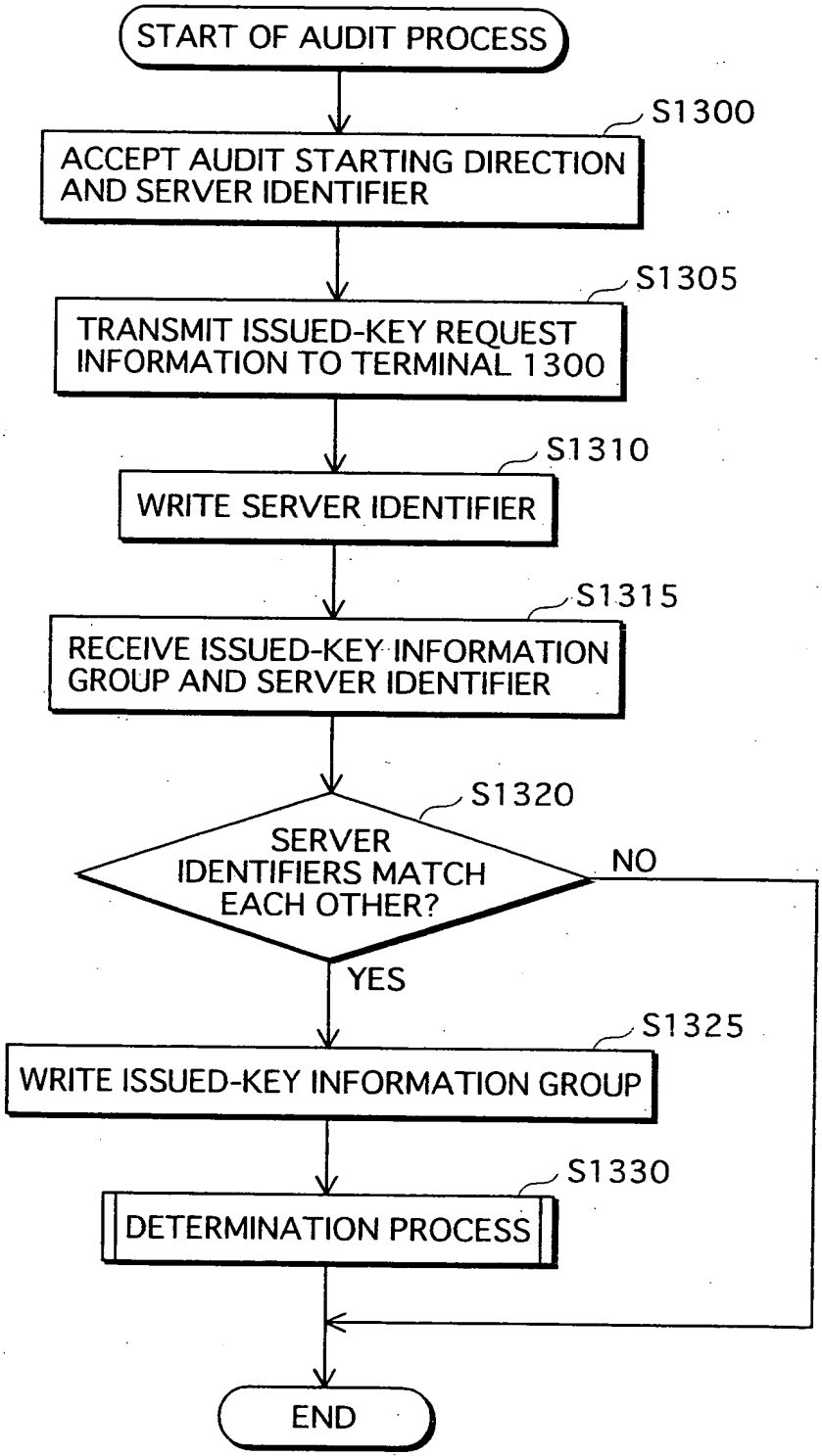

START OF AUDIT PROCESS
S1300
ACCEPT AUDIT STARTING DIRECTION AND SERVER IDENTIFIER
S1305
TRANSMIT ISSUED-KEY REQUEST INFORMATION TO TERMINAL 1300
S1310
WRITE SERVER IDENTIFIER
S1315
RECEIVE ISSUED-KEY INFORMATION GROUP AND SERVER IDENTIFIER
S1320
SERVER IDENTIFIERS MATCH EACH OTHER?
NO
YES
S1325
WRITE ISSUED-KEY INFORMATION GROUP
S1330
DETERMINATION PROCESS
END

FIG.36

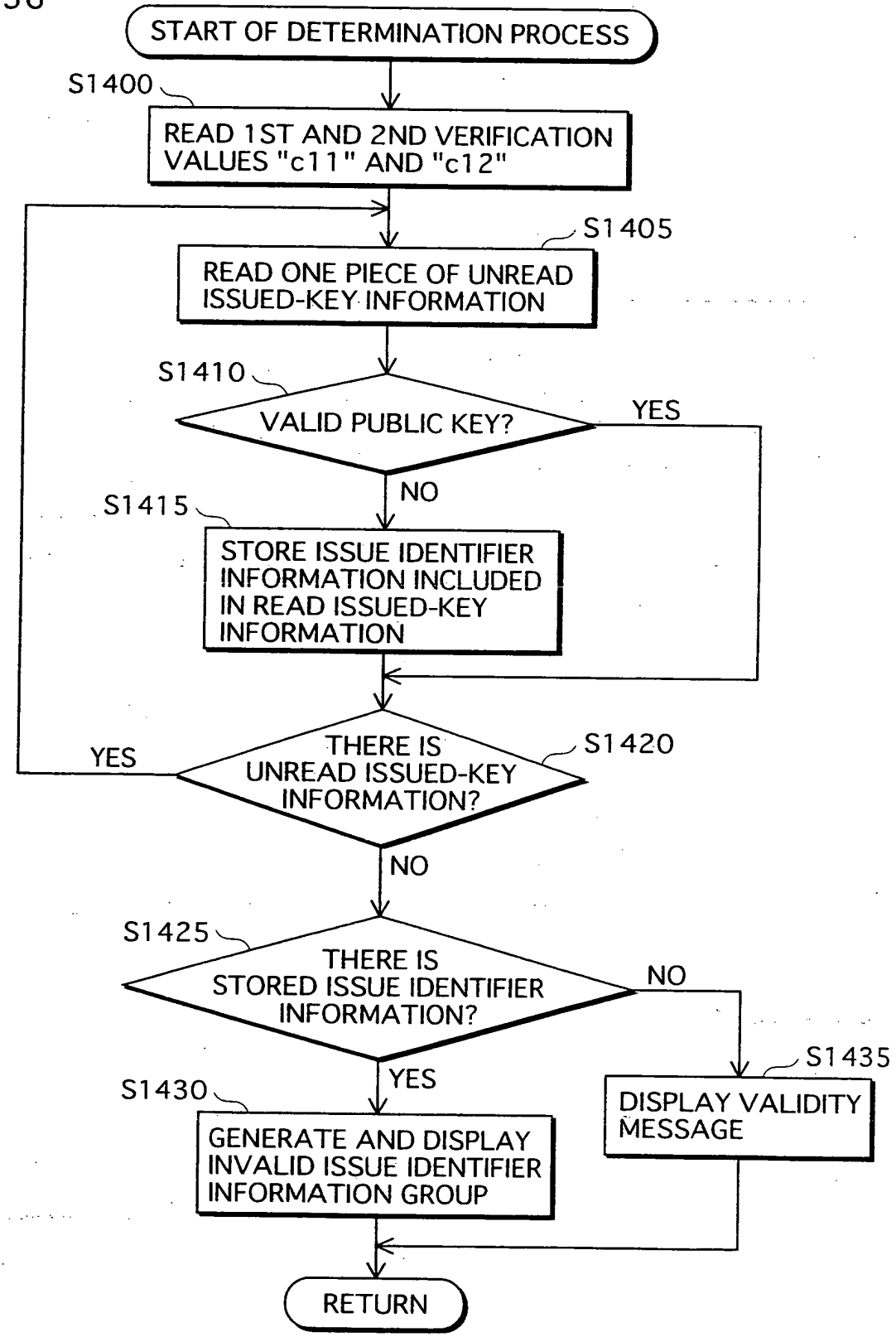

START OF DETERMINATION PROCESS
S1400
READ 1ST AND 2ND VERIFICATION VALUES "c11" AND "c12"
S1405
READ ONE PIECE OF UNREAD ISSUED-KEY INFORMATION
S1410
VALID PUBLIC KEY?
YES
NO
S1415
STORE ISSUE IDENTIFIER INFORMATION INCLUDED IN READ ISSUED-KEY INFORMATION
THERE IS UNREAD ISSUED-KEY INFORMATION?
S1420
YES
NO
S1425
THERE IS STORED ISSUE IDENTIFIER INFORMATION?
NO
YES
S1430
GENERATE AND DISPLAY INVALID ISSUE IDENTIFIER INFORMATION GROUP
S1435
DISPLAY VALIDITY MESSAGE
RETURN

FIG.37

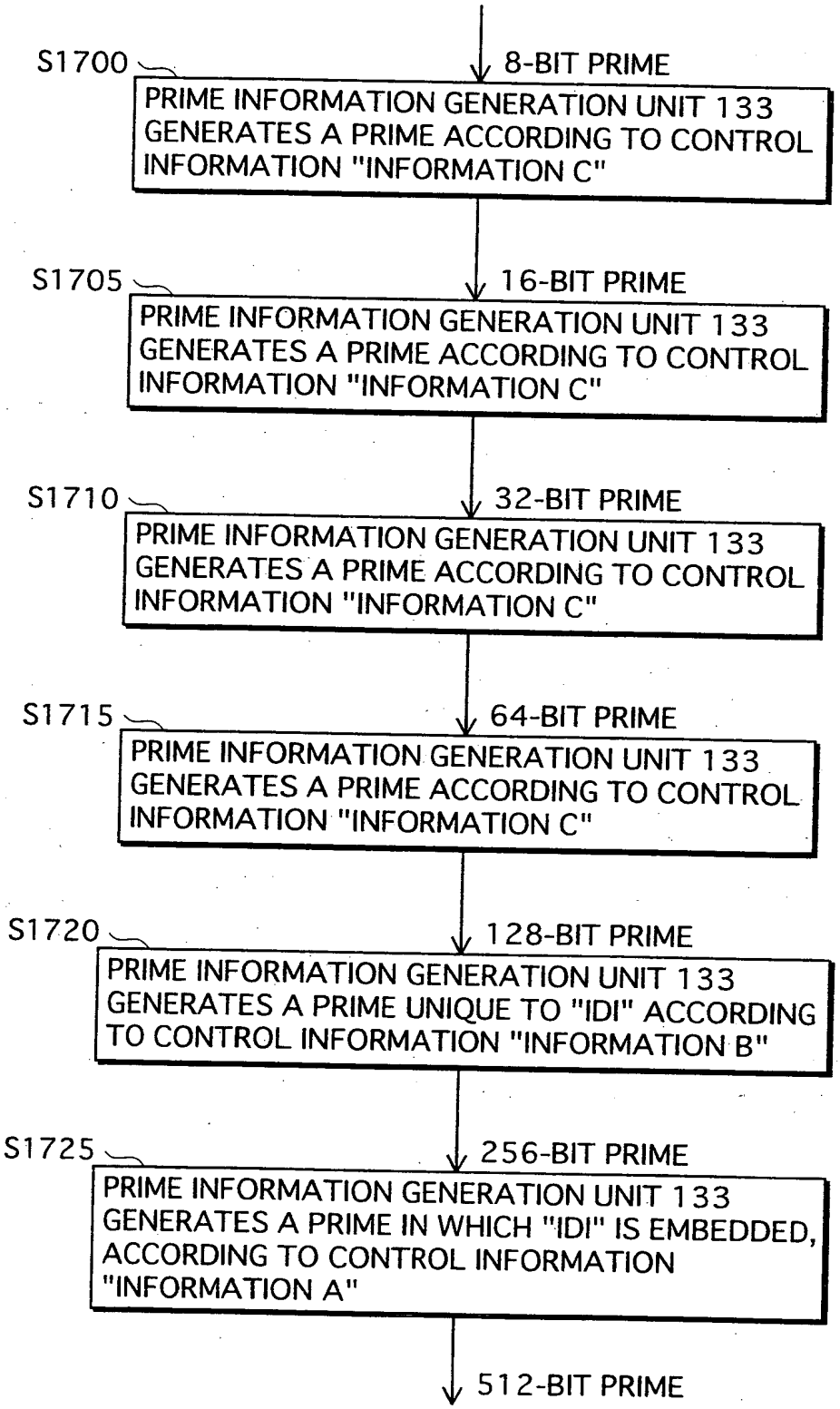

S1700
8-BIT PRIME
PRIME INFORMATION GENERATION UNIT 133 GENERATES A PRIME ACCORDING TO CONTROL INFORMATION "INFORMATION C"
S1705
16-BIT PRIME
PRIME INFORMATION GENERATION UNIT 133 GENERATES A PRIME ACCORDING TO CONTROL INFORMATION "INFORMATION C"
S1710
32-BIT PRIME
PRIME INFORMATION GENERATION UNIT 133 GENERATES A PRIME ACCORDING TO CONTROL INFORMATION "INFORMATION C"
S1715
64-BIT PRIME
PRIME INFORMATION GENERATION UNIT 133 GENERATES A PRIME ACCORDING TO CONTROL INFORMATION "INFORMATION C"
S1720
128-BIT PRIME
PRIME INFORMATION GENERATION UNIT 133 GENERATES A PRIME UNIQUE TO "IDI" ACCORDING TO CONTROL INFORMATION "INFORMATION B"
S1725
256-BIT PRIME
PRIME INFORMATION GENERATION UNIT 133 GENERATES A PRIME IN WHICH "IDI" IS EMBEDDED, ACCORDING TO CONTROL INFORMATION "INFORMATION A"
512-BIT PRIME

FIG.38

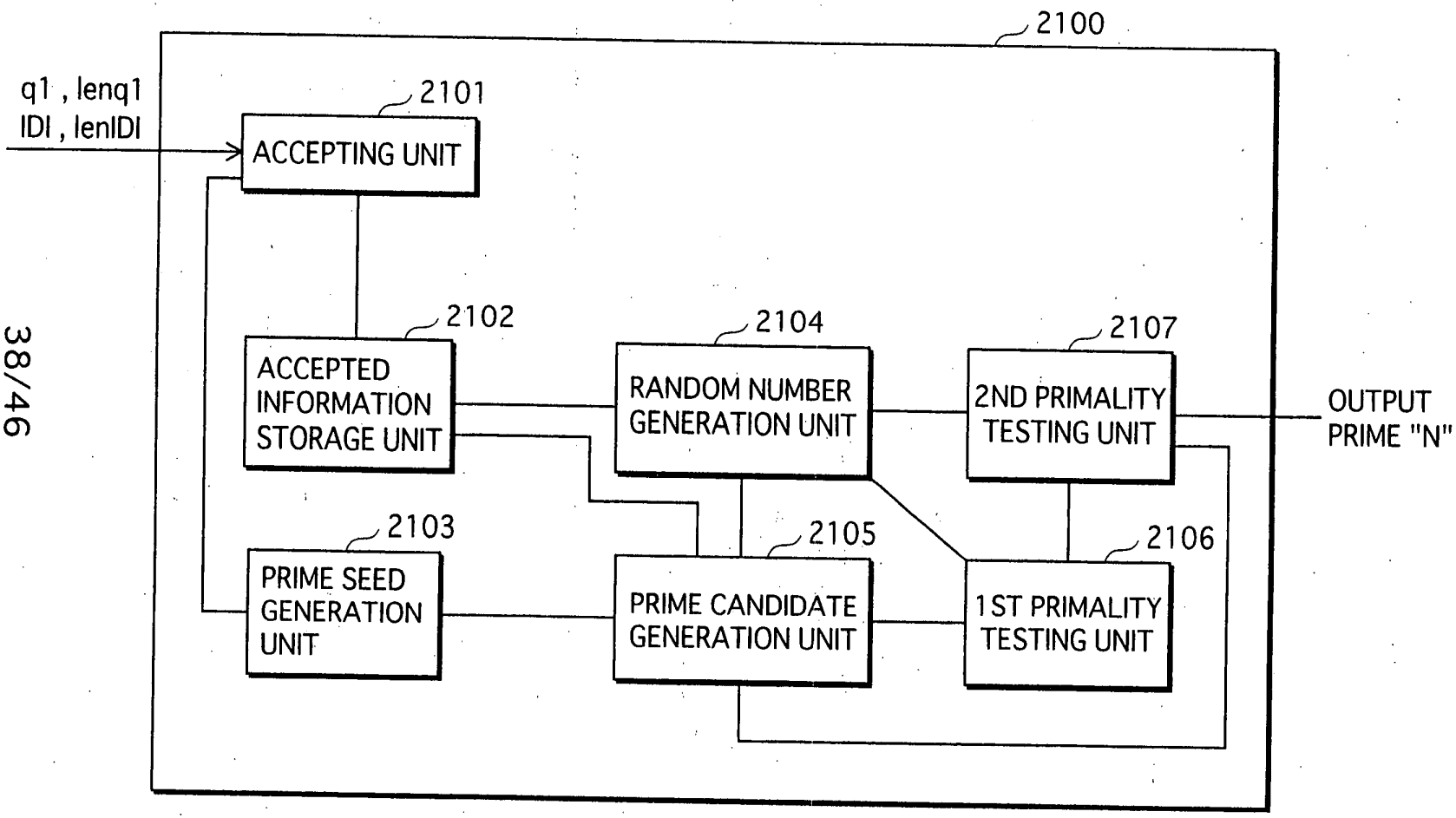

2100
q1 , lenq1
IDI , lenIDI
2101
ACCEPTING UNIT
2102
ACCEPTED INFORMATION STORAGE UNIT
2104
RANDOM NUMBER GENERATION UNIT
2107
2ND PRIMALITY TESTING UNIT
OUTPUT PRIME "N"
2103
PRIME SEED GENERATION UNIT
2105
PRIME CANDIDATE GENERATION UNIT
2106
1ST PRIMALITY TESTING UNIT

FIG.39

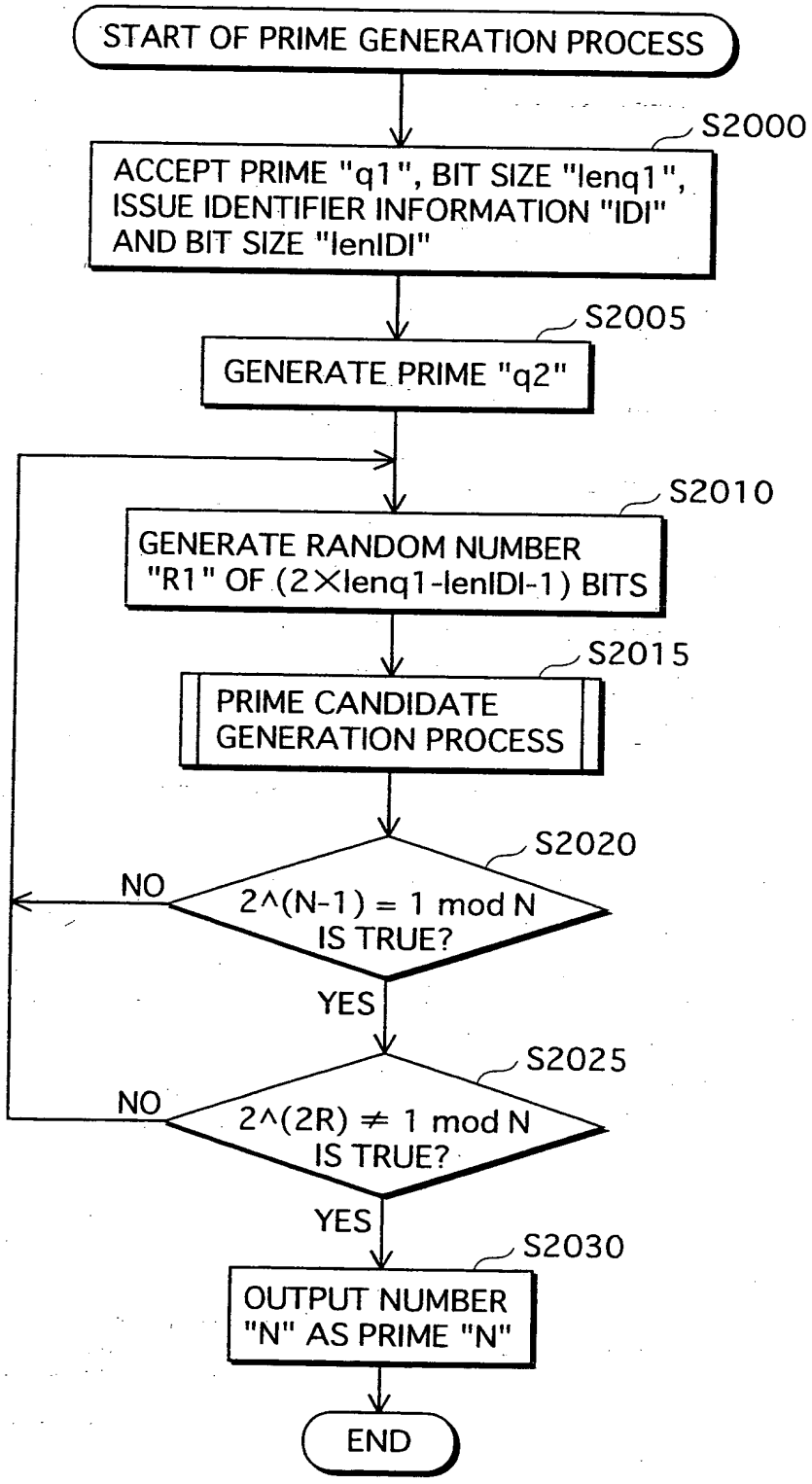

START OF PRIME GENERATION PROCESS
S2000
ACCEPT PRIME "q1", BIT SIZE "lenq1", ISSUE IDENTIFIER INFORMATION "IDI" AND BIT SIZE "lenIDI"
S2005
GENERATE PRIME "q2"
S2010
GENERATE RANDOM NUMBER "R1" OF (2×lenq1-lenIDI-1) BITS
S2015
PRIME CANDIDATE GENERATION PROCESS
S2020
2^(N-1) = 1 mod N IS TRUE?
NO
YES
S2025
2^(2R) ≠ 1 mod N IS TRUE?
NO
YES
S2030
OUTPUT NUMBER "N" AS PRIME "N"
END

FIG.40

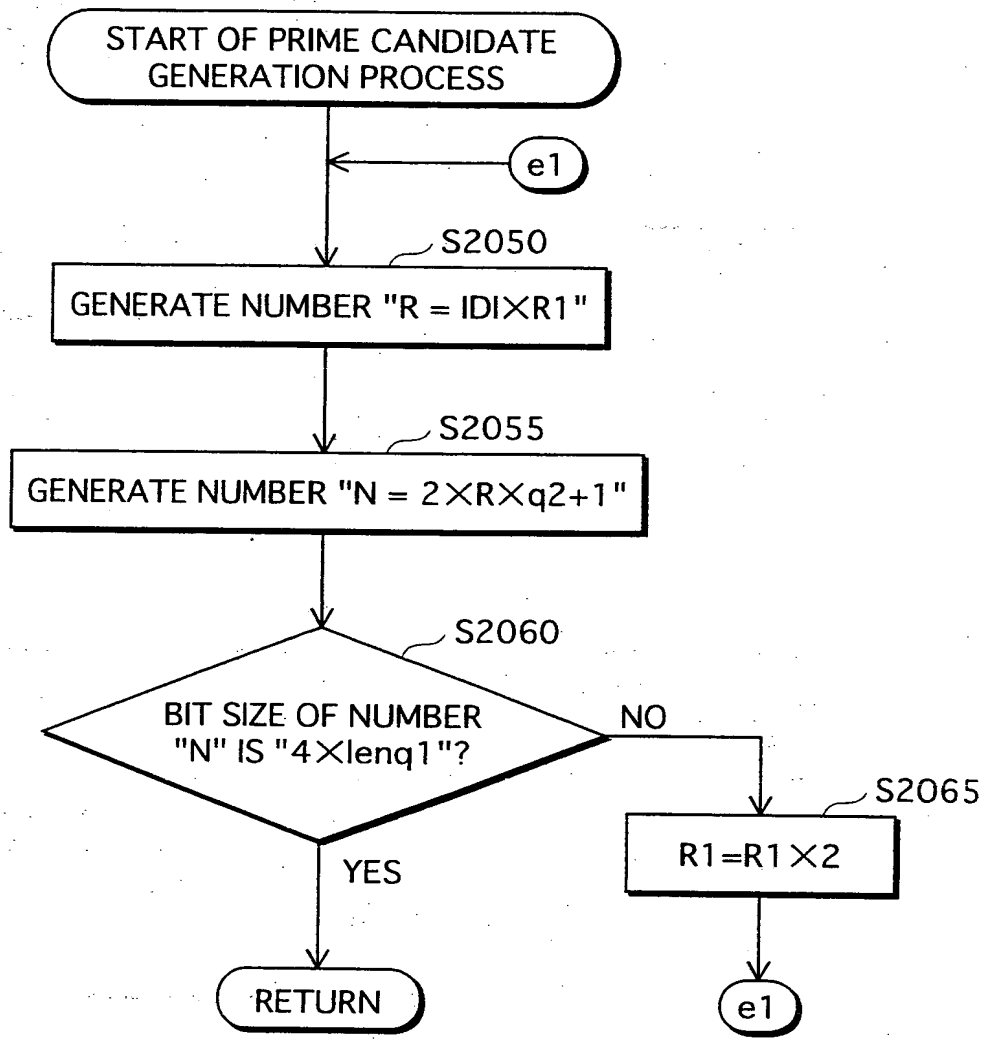

START OF PRIME CANDIDATE GENERATION PROCESS
e1
S2050
GENERATE NUMBER "R = IDI×R1"
S2055
GENERATE NUMBER "N = 2×R×q2+1"
S2060
BIT SIZE OF NUMBER "N" IS "4×lenq1"?
NO
YES
S2065
R1=R1×2
RETURN
e1

FIG.41

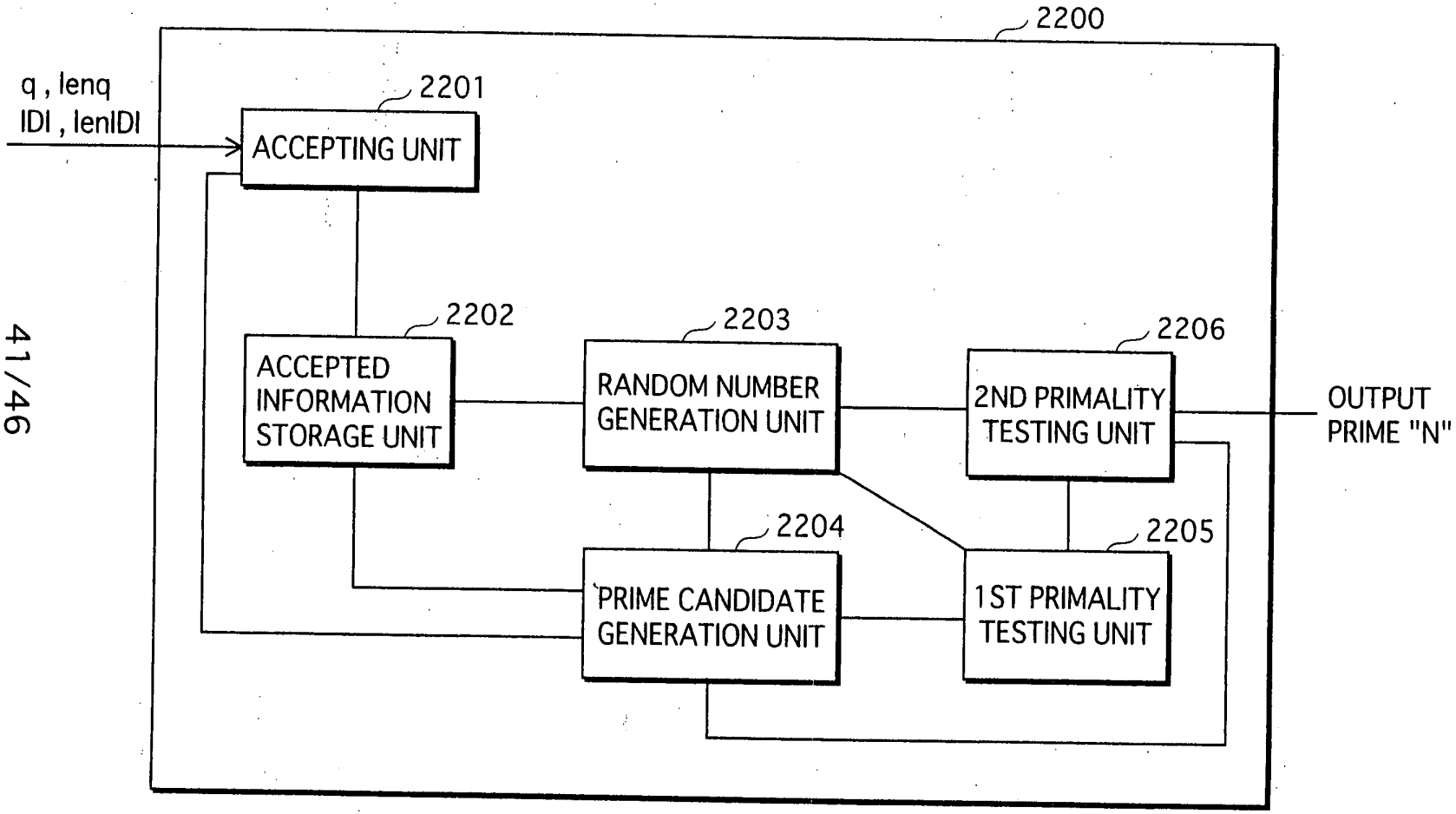

2200
q , lenq
IDI , lenIDI
2201
ACCEPTING UNIT
2202
ACCEPTED INFORMATION STORAGE UNIT
2203
RANDOM NUMBER GENERATION UNIT
2206
2ND PRIMALITY TESTING UNIT
OUTPUT PRIME "N"
2204
PRIME CANDIDATE GENERATION UNIT
2205
1ST PRIMALITY TESTING UNIT

FIG.42

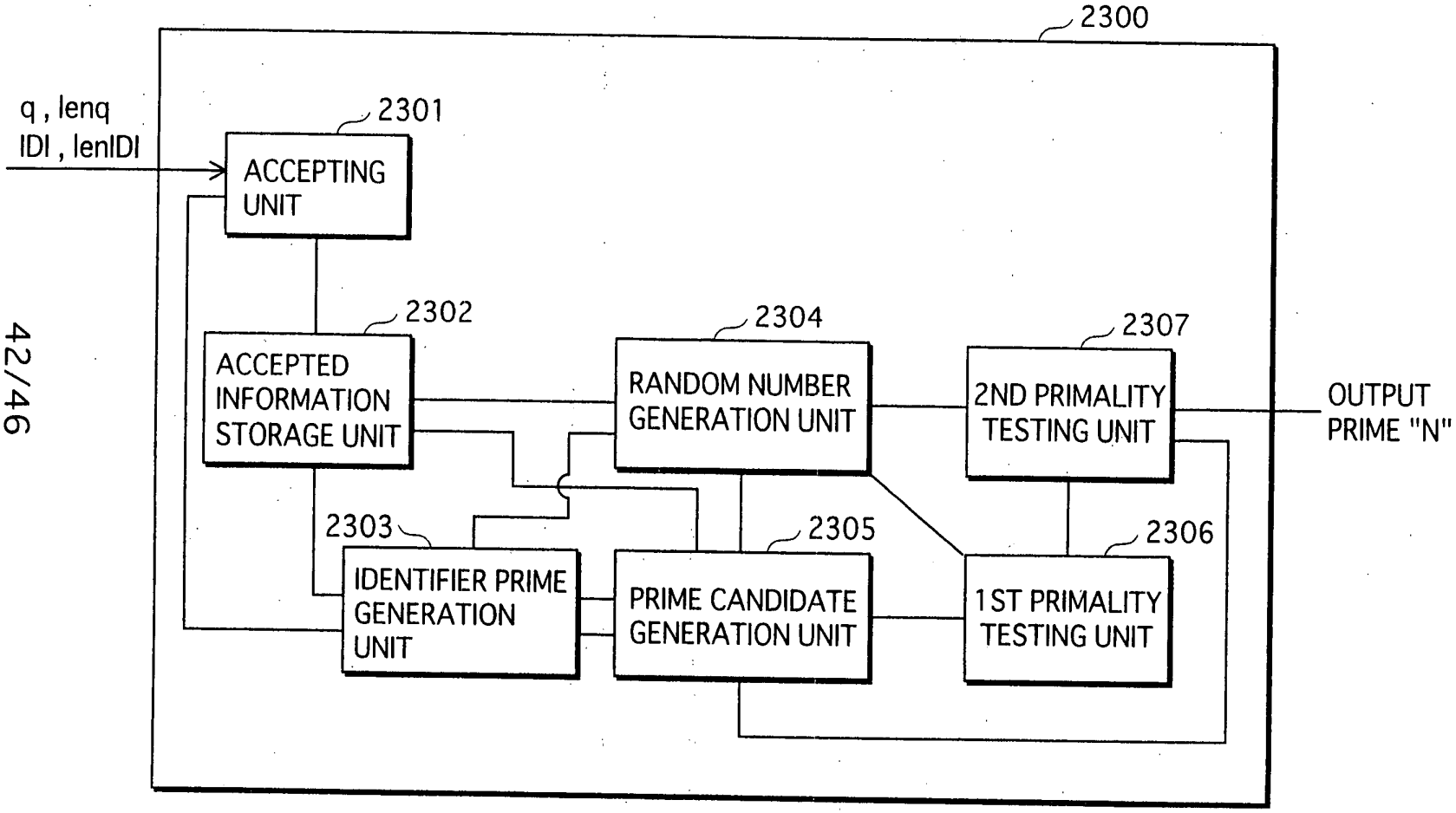

2300
q , lenq
IDI , lenIDI
2301
ACCEPTING UNIT
2302
ACCEPTED INFORMATION STORAGE UNIT
2303
IDENTIFIER PRIME GENERATION UNIT
2304
RANDOM NUMBER GENERATION UNIT
2305
PRIME CANDIDATE GENERATION UNIT
2306
1ST PRIMALITY TESTING UNIT
2307
2ND PRIMALITY TESTING UNIT
OUTPUT PRIME "N"

FIG.43

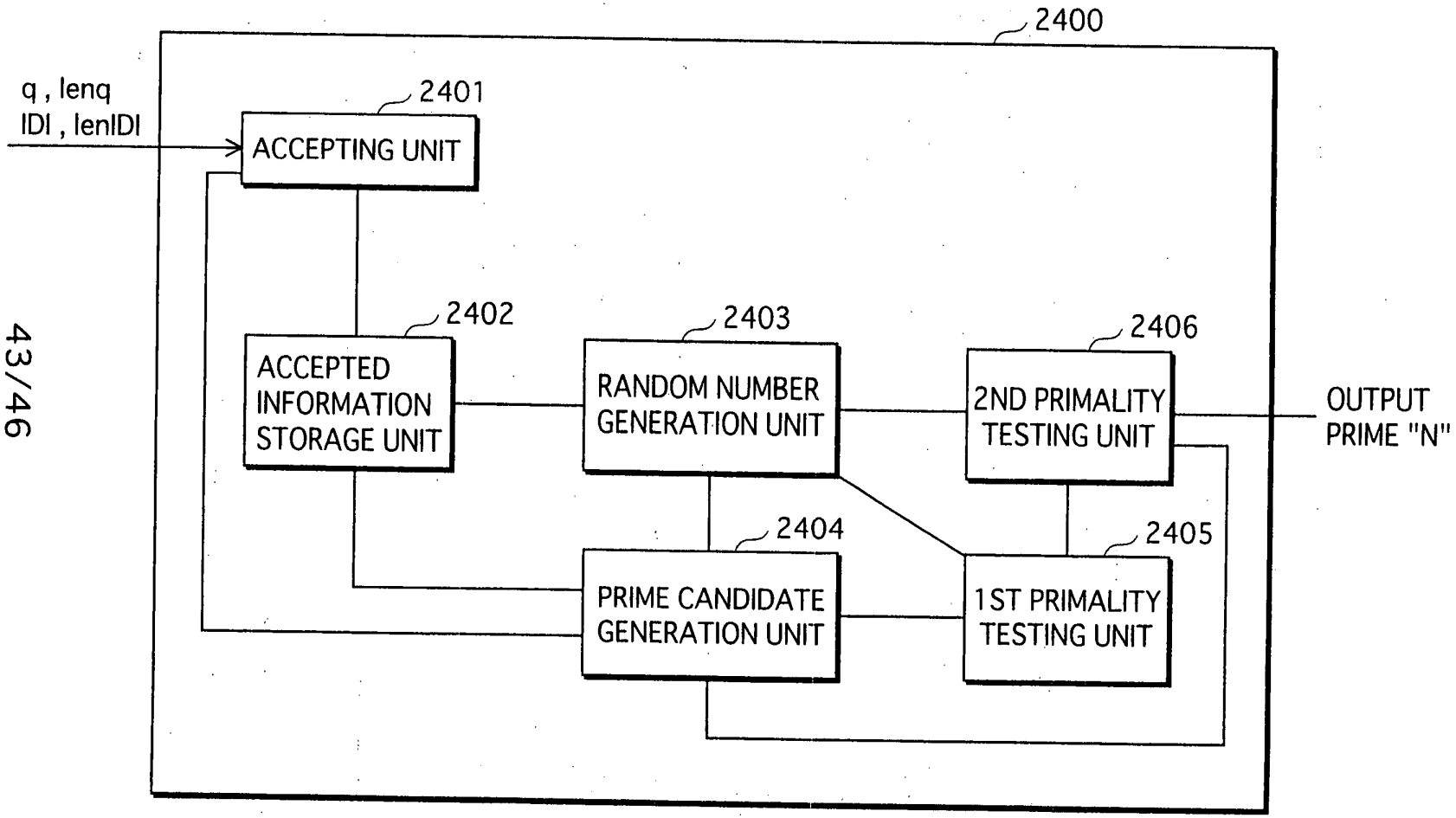

2400
q , lenq
IDI , lenIDI
2401
ACCEPTING UNIT
2402
ACCEPTED INFORMATION STORAGE UNIT
2403
RANDOM NUMBER GENERATION UNIT
2406
2ND PRIMALITY TESTING UNIT
OUTPUT PRIME "N"
2404
PRIME CANDIDATE GENERATION UNIT
2405
1ST PRIMALITY TESTING UNIT

FIG.44

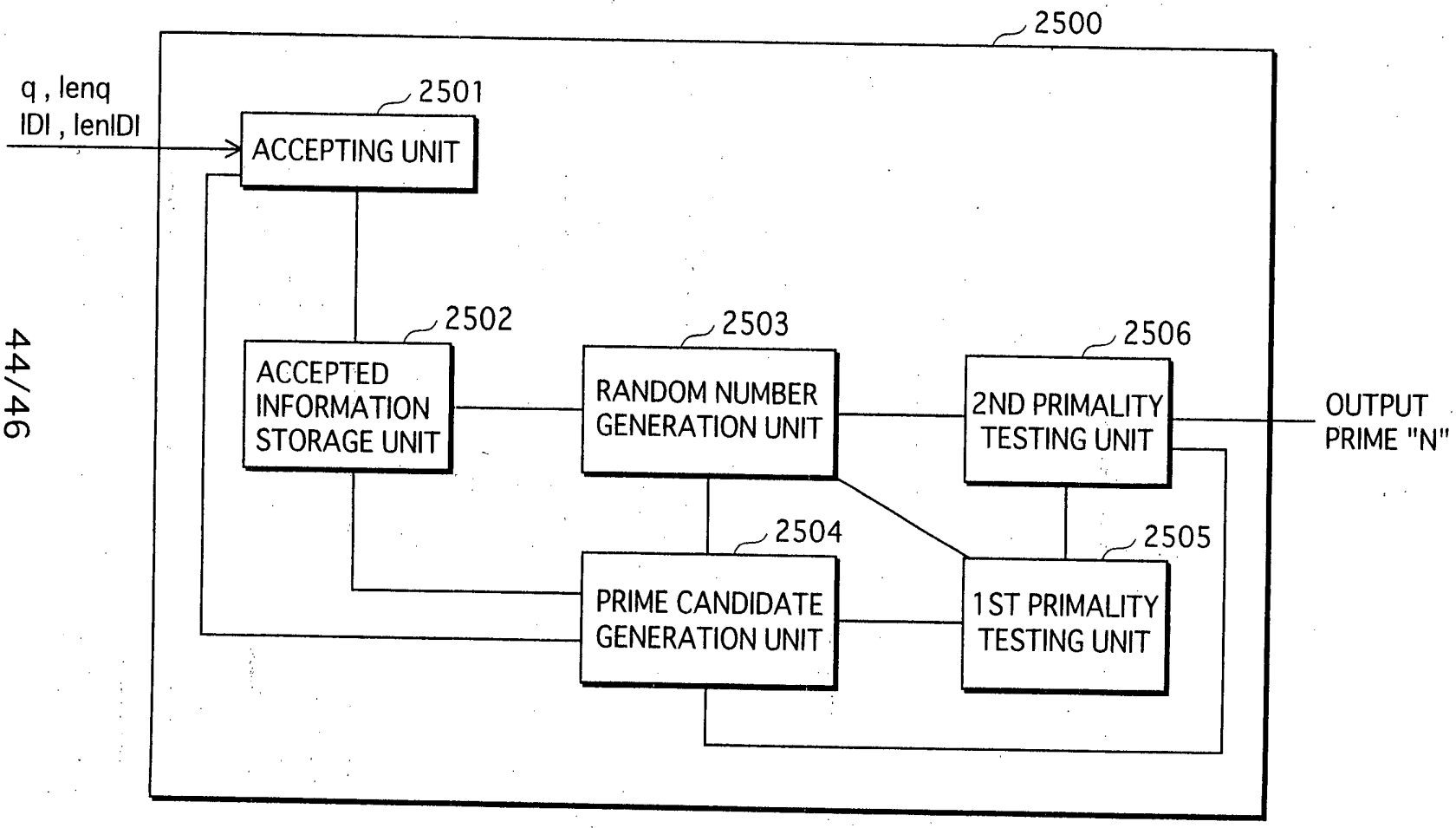

2500
q , lenq
IDI , lenIDI
2501
ACCEPTING UNIT
2502
ACCEPTED INFORMATION STORAGE UNIT
2503
RANDOM NUMBER GENERATION UNIT
2506
2ND PRIMALITY TESTING UNIT
OUTPUT PRIME "N"
2504
PRIME CANDIDATE GENERATION UNIT
2505
1ST PRIMALITY TESTING UNIT

FIG.45

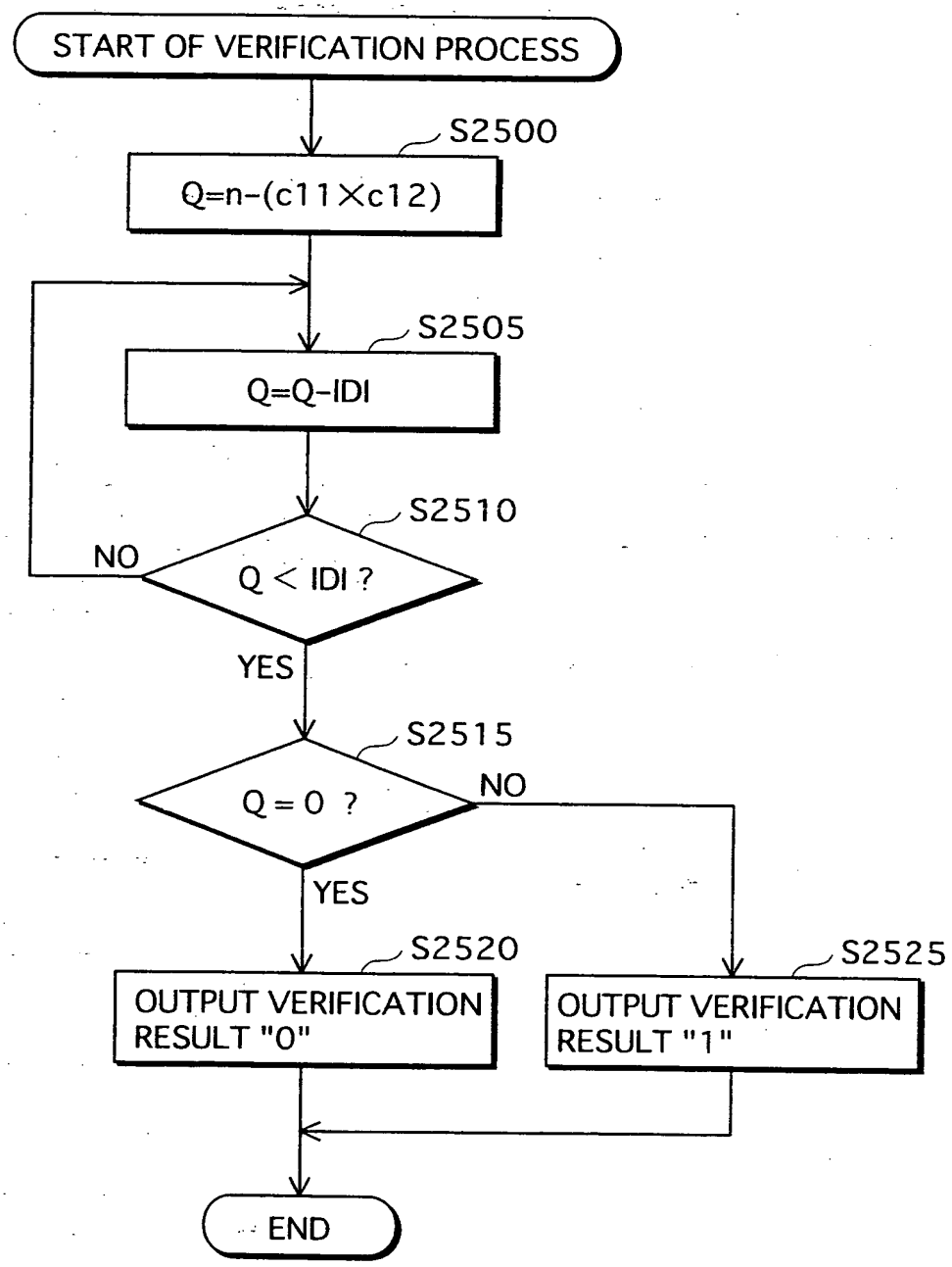
BIT STRING OF ISSUE IDENTIFIER INFORMATION "IDI" : 「$S_1S_2S_3S_4\cdots S_{62}S_{63}S_{64}$」

BIT STRING OF RANDOM NUMBER "R1" : 「$T_1T_2T_3T_4\cdots T_{62}T_{63}T_{64}$」

⇓ GENERATION OF "IDI_R1"

「BIT STRING OF "IDI_R1" : 「$S_1T_1S_2T_2S_3T_3S_4T_4\cdots T_{61}S_{62}T_{62}S_{63}T_{63}S_{64}$」

FIG.46


START OF VERIFICATION PROCESS
S2500
Q=n-(c11×c12)
S2505
Q=Q-IDI
S2510
NO
Q < IDI ?
YES
S2515
Q = 0 ?
NO
YES
S2520
OUTPUT VERIFICATION RESULT "0"
S2525
OUTPUT VERIFICATION RESULT "1"
END